IoT Security: A Layered Approach for Attacks & Defenses

Mian Muhammad Ahemd
Department of Computer Science
COMSATS Institute of Information Technology Islamabad, Pakistan
mianfixture@gmail.com

Munam Ali Shah
Department of Computer Science
COMSATS Institute of Information Technology Islamabad, Pakistan
mshah@comsats.edu.pk

Abdul Wahid
Department of Computer Science
COMSATS Institute of Information Technology Islamabad, Pakistan
abdulwahid@comsats.edu.pk

***Abstract*—Internet of Things (IoT) has been a massive advancement in the Information and Communication Technology (ICT). It is projected that over 50 billion devices will become part of the IoT in the next few years. Security of the IoT network should be the foremost priority. In this paper, we evaluate the security challenges in the four layers of the IoT architecture and their solutions proposed from 2010 to 2016. Furthermore, important security technologies like encryption are also analyzed in the IoT context. Finally, we discuss countermeasures of the security attacks on different layers of IoT and highlight the future research directions within the IoT architecture.**

Keywords*— *Internet of Things; IoT; Security; layer architecture;

I. INTRODUCTION

The IoT [1] emerges as a new concept in future Internet when the physical objects become the part of Internet. IoT provides objects the unique identity accessible from the network and its status, location can be track down[2]. Many facilities such as tracking monitoring and controlling become possible with the IoT which changes the human interactions with the physical objects. There are many devices developed which are now used as the IoT such as, RFID (Radio Frequency Identification Devices), infrared sensors, laser scanner, GPS (Global Positioning System) and gas inductors. In IoT various parameters of the objects or processes such as sound light mechanics, chemistry, biology, and position can be monitored and controlled. The great thing about IoT is that all the information is based on real time data.

IoT comprises of a network of highly diverse digital objects interacted with each other and with humans too. It provides a sensor network with communication system, store and manage the information, provides access and also handles the privacy protection and data security problems [3]. Comparing the research aspects on security in IoT to security in Internet, former is the way complex than the later and therefore needs the significant attention of the researcher and a more precise research methodology and tools should be incorporated. With respect to security, IoT can be divided into four layers[4] [5] [6]. As shown in figure 1.

A. *Perception layer:*

This layer utilizes the different sensors such as ZigBee, infra-red, RFID and QR code to collect information. Information could be temperature, humidity, vibration, force, pH level pressure, speed etc. Transmission of information collected is carried out through network layer to central information processing unit.

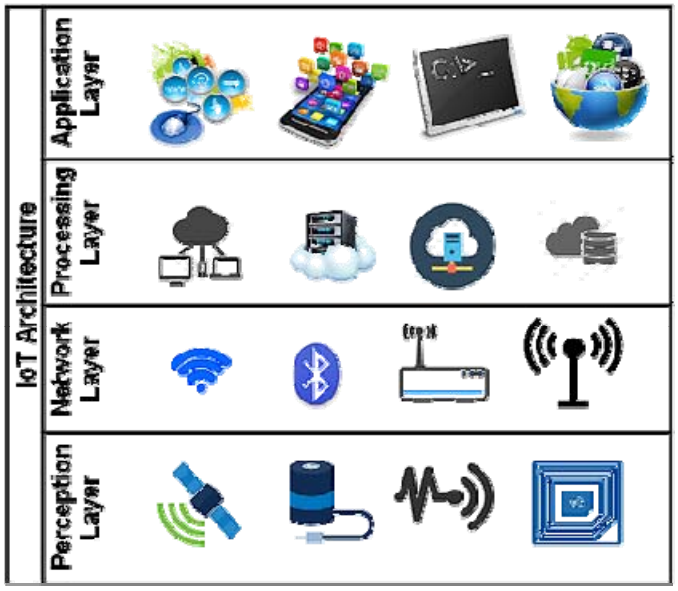

Figure 1: IoT Layers

B. *Network Layer:*

The transmission of information is carried out in this layer. Information transmitted through the different mediums such as RFTD, Infrared, satellite and Wi-Fi units depending upon the nature of sensors and sensitivity of data. Hence data transmits securely from perception layer to other layers through network layer.

C. Processing layer:

This layer works to combine the network layer and application layer. All the intelligent and cloud computing is done in this layer. Support layer functionality includes storage of data from lower level layers to data base and service management. On the bass of intelligent computing this layer can compute information and process data automatically.

D. Application layer:

Application layer provides services as per user demand. The processed information of the lower layers is utilized to produce useful services for end user. The information provides a platform for such applications which could benefit the user in many ways such as health education personal use, gadgets, household, transportation, communication etc. The information security in IoT should be equipped with feature like confidentiality, identification, etc. As IoT is going be applied in different important fields like health, transportation, industries, smart homes, postal services, etc. thus the security and privacy of IoT should be fool proof. Targeted solution to each security factor should be defined.

In this paper we discuss the four layered architecture of IoT and their security. We discuss different security features and security challenges of these layers. And on the bases of former research we discuss different security aspects like cryptography, communication security, protecting sensor data and outline the challenges briefly. Rest of the paper is organized as follow. Section II provides a brief overview of the security threats of each layer and their countermeasure. In Section III, performance evaluation is done on the basis of the literature. Section IV provides the work directions which are needed to be done in feature and in Section V, the work done in the paper is concluded.

II. LETRATURE REVIEW

In this section, we discuss different security threats and their countermeasure on each layer briefly which have been purposed recently.

A. Preception Layer Attacks

Hardware attacks are the most common attacks on perception layer. Perception layer generally includes WSN, RFID, zigbee and other kind of sensors. The attacker needs to be in the network or physically close to the nodes of the IoT system. Some of the common attacks on the perception layer are listed below.

- *Hardware Tempering*

Attacker physically close to the nodes can damage the node by changing the parts of its hardware or completely replacing that node [8]. Changing the electronic integration or by capturing the gate way node, the attacker can get all the information on that network including routing table, communication key, cryptographic key, radio key etc and threat all the network including higher layers.

- *Fake node injection*

The attacker can inject a fake or malicious node between the nodes of the network [7], hence the attacker gain access to the network and be able to control all the data flow of the network. It can make the node to stop transmitting the real data and hence destroy the entire network.

- *Malicious code injection*

The nodes of the IoT network can also be compromised by injecting malicious code. Dos attacks in WSN or virus on to the nodes are the most common type of this attack [9]. By this attack the attacker can gain access to the network, and can make the network to lose resources and hence make the services unavailable.

- *Sleep denial attack*

Node on the remote places in IoT network are mostly powered by replaceable batteries, the nodes are programmed to sleep when they are not in use to increase their battery life[10]. In this attack the attacker keep the node awake and prevent them to fell asleep by feeding wrong input to the node which results in power consumption hence the node shutdown.

- *WSN Node Jamming*

Wireless sensor network works on the radio frequency. A denial of service can be created by sending the noise signals over the network or by jamming the signals of WSN. This deny the communication between the nodes of the IoT network. The attacker keep on jamming the signals which result in the denial of services of the IoT [11].

- *RF interference of RFIDs*

RFIDs also works on radio signals as mentioned in WSN network earlier. The difference is that attacker don't need to jam the signals, the attacker can create make the nodes to deny the services just by sending noise signals over the network[12]. This noise interferes the RFID signal which create a hurdle in communication of the nodes.

B. Preception Layer Attacks Countermeassures

- *Authentication*

To keep malicious devices out of the IoT network authentication of the devices should be done before getting into the network[13]. Without proper authentication the device should not be allowed to communicate with the network which prevents false data flow in the network.

- *Data integrity*

Each device in the IoT network should be provided by error detection mechanism, which minimizes the risk of data tempering. There are different error detection mechanism which being used like parity bit, check sum, etc. To make it more secure, cryptographic hash function should be used[14].

- *Secure booting*

Cryptographic hash algorithm can be used to check integrity and the authentication of the software on different devices of the IoT network. But in most cases the end devices of the network possess very low computing power. So, most of the

hash algorithms cannot be implemented on these devices. WH and NH cryptographic algorithms are the best solution to this problem because they need very low processing to execute [15].

- *IPSec Security channel*

IPSec security provides two kinds of security features, authentication and encryption. Eavesdropping and data tempering can be avoided encoding the data which insure data confidentiality[16]. The sender of the data can be identified by the receiver that's the sender over the IP is real or not.

- *Anonymity*

The inject node in the network by the attacker can hide sensitive information like location, identity etc. These kinds of the nodes are sensed anonymous by the network. Solution to this problem is presented as k-anonymity approach [17]. This approach work very best on low processing devices.

- *Physical secure design*

To resolve most of the attacks of perception layer can be resolved by designing the end devices physically secure. It includes chip selection, radio frequency circuits, data acquisition unit design, etc. These components should be of high quality and should not be easily changeable. The design of antenna for wireless communication should be able to communicate over good distance[18].

C. Network Layer Attacks

The attacks are targeted to IoT system network. Such attacks can be performed without being close to the network.

- *Traffic analysis attacks:*

The wireless technologies of transmission are sniffed to obtain confidential information such as RFID. In such cases hacker first obtain information related to network by using packet sniffers or port scanning application and then attacks on the targeted information[19].

- *RFID Spoofing*

In RFID spoofing attacker targets the RFID signal to gain access the information imprinted on RFID tag[20]. Once the signal spoofed hacker uses it to transmit his own data using the original id. Now hacker obtained the full access to system.

- *RFID unauthorized access*

As there is no secured authentication system in RFID systems, the tags are accessible to anyone. It means tags can be manipulated easily[21].

- *Sinkhole Attack*

The attack directs all signals from wireless sensor network nodes to a same point. Such attack voids the data safety and drops all the packets instead of delivering to its destination[22].

- *Man in the Middle Attack*

Web attacker interfere the two sensor nodes to access restricted information and violates the privacy of nodes[23]. Such attack doesn't demand the attacker to be physically appeared on the location of network. This can be done by using the communication protocol of the IoT.

- *Routing Information Attack*

These are immediate attacks that the enemy by spoofing, replaying or changing routing data can convolute the system and make routing loops, permitting or dropping movement, sending the false error messages, shortening or amplifying source courses or notwithstanding parceling the network[24].

D. Network Layer Attacks Countermeassure

- *Data privacy*

Data privacy in the IoT can be achieved by preventing illegal access of the nodes of the network. Different authentication mechanism can be used for this purpose, one of them is point to point encryption[25]. In this method the confidential data is converted immediately to a code which is indecipherable

- *Routing security*

Secure routing is the key to the secure utilization of sensor systems for some applications, yet the larger numbers of routing conventions are unstable. Routing security for the sensor network can be ensured by routing the data through multiple paths which increase error detection of the network[26].

- *Sinkhole attack*

Attack which is from outside the network can be secured by encryption and authentication, so the attacker not be able to join the network. And the attack from inside the network can be secured by security aware ad hoc routing protocol (SAR)[27]. Ssecurity metrics is added to the packets of route request, after analyzing the received data the attacker can be dropped from the network.

- *Spoofing*

Spoofing attack can be encountered by GPS location system. In[28] the GPS system techniques has been described and implemented. It is not the perfect solution but it is one the best solution provided yet.

- *Data integrity*

Data integrity can be achieved by applying cryptographic hash functions on the data[29]. This ensures data is not tempered when it reaches the receiving end. Mitigation problem can be resolved by applying error correction mechanism.

E. Processing Layer Attacks

Cloud attacks are the most common type of attacks in processing layer of IoT because the data is sent to the cloud at this phase. So we discuss some common attacks which can make the network vulnerable to threats.

- *Application security*

Most of the application on cloud SAAS are delivered through internet i.e. web services. An attacker can easily uses web to get into the IoT network and can steal the data or can perform

malicious activities. Security issues in SAAS are much different from usual web securities issues. OWASP had identified different security issues on SAAS [30].

- *Data security*

Data security is the major concern of a SAAS user. It's the responsibility of the SAAS provider to ensure the security, the data processed and stored on cloud as plan text. The major security issues occur on the facilitation of data backup provided by the service provider [31]. Data back is offered through third party in most of the cases which increase the treat of data theft.

- *Underlying infrastructure security*

In PaaS, lower layers of IoT are not accessible to the developer, underlying layer's security is the responsibility of the provider[32]. Even developer can develop a secure application but its security remain vulnerable due to lower layers of IoT.

- *Third-party relationships*

PaaS not only provides programming language, it also provide third party web service component i.e. mashups[33]. More than one source is combined in mashups which increase security issues like network and data security.

- *Virtualization threats*

Security of virtual machines is as important as the security of the physical machines and any defect in possibly one may influence the other[34]. Virtualization in processing layer is vulnerable to many types of attacks.

- *Shared Resources*

As virtual machines share same resources, this becomes a security threat to the network. Using covert channels an attacker can monitor all the shared resources between the virtual machines so the information might be compromised[35].

F. Processing Layer Attacks Countermeassure

- *Fragmentation redundancy scattering(FRS)*

In data FRS the sensitive data on the cloud is divided into different fragments and stored on different servers [36]. The fragments of the data don't have any significant information by itself, so the risk of data leakage is minimized.

- *Homomorphic encryption*

This method is based on full homomorphic encryption application. This method allows cipher texts to be computed arbitrarily without being decrypted. This method requires high computation but assure data security[37].

- *Web application scanners*

Web application scanner is program proposed in [38] which detect treats from the front end of the web. There are other web firewall applications which can detect a potential attacker.

- *Hyper Safe*

Hypersafe lockdowns and protects the write protected memory pages from being modified, pointing index is restricted that converts controlled data into the pointer indexes[39].

- *Encryption*

Encryption is used for securing the sensitive data. Data sent or stored on the cloud is in encrypted form. There are different type of encryption mechanisms like Advanced Encryption Standard etc[40]. It can also help in overcoming side channels attack.

G. Application Layer Attacks

Before In computer security, amenability of security is caused by software attacks. By using Trojan horse programs, worms, viruses, spyware and malicious scripts software attacks can develop the system that can harm IoT System devices, appropriate information, tamper with data and deny service.

- *Phishing Attacks*

From spoofing the user's conformation ID, confidential data can be accessed by attacker through contaminated web site or email[41].

- *Virus, Worms, Trojan Horse, Spyware*

System can be contaminated by opponents with nasty software that can results in pinching information, tampering data or even denial of service[42].

- *Malicious Scripts*

IoT network is generally associated with Internet. Entire system closes up and data stealing is caused by running executable active-x scripts take in by the user that reins the access[43].

- *Denial of Service*

Through application layer, IoT network can be exaggerated by the execution of DoS or DDoS attacks by the attackers that influence the users on the network. Genuine users can be infertile by these attacks and attackers can obtain complete access on application layer, databases and private sensitive data[44]

- *Data Protection and Recovery*

User privacy is involved in communication data. Data can be lost and even catastrophic damage can be caused imperfect algorithms and mechanisms of data processing and data protection[45]. The mass nodes management is also one reason.

- *Software Vulnerabilities*

Vulnerabilities occur due to the non standard code as it was written by programmers, as a result buffer runoff. This technique or method is used by the hackers to accomplish their rational[46].

- *Data security*

User privacy is involved in communication data. Data can be lost and even catastrophic damage can be caused imperfect algorithms and mechanisms of data processing and data

Table 1. Comparative Analysis

Layers	Attack Name	Attack References	Effects	Launch	Countermeasure	Countermeasure reference
Perception Layer	Hardware Tempering	[8]	Data leakage (Keys, routing tables, etc)	2011	Secure Physical Design	[13]
	Fake node injection	[7]	Fake Data Manipulation	2013	Secure Booting	[14]
	Malicious code injection	[9]	Halt Transmission	2012	Intrusion detection Technology(IDT)	[15]
	Sleep denial attack	[10]	Node shutdown	2012	Authentication	[16]
	WSN Node Jamming	[11]	Jam Node Communication	2010	IPSec Security channel	[17]
	RF interference of RFIDs	[12]	Distortion in node Communication	2012	Authentication	[18]
Network Layer	Traffic analysis attack	[19]	Data leakage (about network)	2013	Routing Security	[26]
	RFID Spoofing	[20]	Intrusion in network Data manipulation	2011	GPS Location System	[28]
	RFID unauthorized access	[21]	Node data can be modified (Read, Write & Delete)	2014	Network Authentication	[25]
	Sinkhole Attack	[22]	Data leakage (Data of the Nodes)	2013	Security Aware AdHoc Routing	[27]
	Man in the Middle Attack	[23]	Data Privacy Violation	2011	Point-to-Point Encryption	[29]
	Routing Information Attack	[24]	Routing loops (Network Destruction)	2011	Encrypting Routing Tables	[30]
Processing Layer	Application security	[30]	Privacy Violation	2014	Web Application Scanner	[37]
	Data security	[31]	Data leakage (User data on cloud)	2012	Homomorphic Encryption	[33]
	Underlying infrastructure security	[32]	Service Hijacking	2010	Fragmentation redundancy scattering	[38]
	Third-party relationships	[33]	Data Leakage (User data on cloud)	2013	Encryption	[39]
	Virtualization threats	[34]	Resources destruction	2012	Hyper Safe	[38]
	Shared Resources	[35]	Resources Theft	2011	Hyper Safe	[38]
Application Layer	Phishing Attacks	[40]	Data Leakage (User credentials data)	2016	Biometrics Authentication	[47]
	Virus, Worms, Trojan Horse, Spyware	[41]	Resource Destruction & Hijacking	2012	Protective Software	[48]
	Malicious Scripts	[42]	Hijacking	2011	Firewalls	[49]
	Denial of Service(DoS)	[43]	Resource Destruction	2010	Access Control Lists	[50]
	Data Protection and Recovery	[44]	Data loss & Catastrophic Damage	2011	Cryptographic Hash Functions	[46]
	Software Vulnerabilities	[45]	Buffer over flow	2011	Awareness of security	[51]

protection[47]. The mass nodes management is also one reason

H. Application Layer Attacks Countermeassure

- User *Authentication*

Encryption and Integrity mechanisms are significant for the privacy and protection of system beside data stealing; as a result unauthorized access and data of the system can be protected[48].

- *Access Control Lists (ACLs)*

For accessing and controlling the IoT system, special policies and permissions are made. Incoming or outgoing traffic and access request of network can be allowed or blocked by ACLs[49].

- *Firewalls*

If the password is weak, the password of authentication and encryption can be break. Packets can be filtered, blocked that are not required, unfriendly login attempts, and DoS attacks before even authentication process begins by using the firewall[50].

- *Anti-virus, Anti-spyware and Anti-adware*

For the security, confidentiality, reliability and integrity of IoT system these software are essential.

- *Risk Assessment*

Application layer can be secured by risk assessment in risk assessment technique continuously detects threats of the system, apply patches and updates of the firmware of the system devices which improve security of the system[51]

III. Performance Evaluation

In this section, we have evaluated security threats on the layers of IoT network and presented their countermeasures. We have combined different types of attacks, their names, the name of layer on which that specific attacks are carried out. Furthermore, we have also highlighted the effects of these attacks on the IoT network or the compromise that we have to make if these attacks are launched. Launching periods of these attacks are also discussed and separate countermeasures of all the attacks are presented, applying which, we can minimize the damages that these attacks may do. The detail of our performance evaluation can be seen in table 1. The table classifies the attacks and preventive measures in such a way that it is easy to identify the type of attack and its solution to limit the attackers from damaging the IoT network.

IV. Discussion and Open Challenges

By the year 2025 hundred millions devices are to be connected in the IoT. So the security of the network should be the most important issue in upcoming days. The security is becoming a challenge because there is no standard architecture and security strategies implemented for one architecture might not be feasible for another, as a result probability of security attacks increases. So, the need for a standard architecture for IoT is mandatory. Nodes in an IoT network are not capable enough to handle complex security algorithms like Cryptography etc hence there is a strong need for some algorithms that can be implemented on these low-processing devices.

V. Conclusion

IoT has been a hot research topic for the last few years and like other revolutionary technologies, it also faces many challenges, most significant of which are the security and privacy threats. In this paper, we described the working of four layers of IoT (Perception Layer, Network Layer, Processing Layer and Application Layer) and then we explored the security loopholes that can be exploited in these layers. Furthermore, we explained the countermeasures that can be adopted to prevent and secure the IoT network from the security threats. Moreover, we also suggested some improvements in the IoT network to make it more secure and to overcome the deployment issues. As IoT is going to be a vital part of our daily lives in the near future, extraordinary steps must be taken to ensure that users trust and privacy.

References

[1] F. Xia, L. T. Yang, L. Wang, and A. Vinel, "Internet of Things," *Int. J. Commun. Syst.*, pp. 1101–1102, 2012.

[2] L. Coetzee and J. Eksteen, "The Internet of Things – Promise for the Future ? An Introduction," in *IST-Africa*, 2011, pp. 1–9.

[3] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of Things : Security Vulnerabilities and Challenges," in *International Workshop on Smart City and Ubiquitous Computing Applications*, 2015, pp. 180–187.

[4] J. Xu and Y. Geng, "Security Characteristic and Technology in the Internet of Things," *J. J. Nanjing Univ. Posts Telecommun. (Natural Sci.*, 2010.

[5] S. Kraijak and P. Tuwanut, "A Survey On Internet Of Things Architecture , Protocols , Possible A Pplications , Security , Privacy , Real-World Implementation And Future Trends," in *ICCT*, 2015, pp. 26–31.

[6] H. Suo and J. Wan, "Security in the Internet of Things : A Review," *Int. Conf. Comput. Sci. Electron. Eng.*, p. 4, 2012.

[7] K. Zhao and L. Ge, "A Survey on the Internet of Things Security," *Ninth Int. Conf. Comput. Intell. Secur.*, 2013.

[8] D. E. Burgner, "Security of Wireless Sensor Networks," in *Eighth International Conference on Information Technology: New Generations*, 2011.

[9] T. Halim, "A Study on the Security Issues in WSN," *Int. J. Comput. Appl.*, vol. 53, no. 1, p. 8887, 2012.

[10] T. Bhattasali, "Sleep Deprivation Attack Detection in Wireless Sensor Network," *Found. Comput. Sci. New York, USA*, 2012.

[11] M. Li and I. Koutsopoulos, "Optimal Jamming Attack Strategies and Network Defense Policies in Wireless Sensor Networks," *IEEE Trans. Mob. Comput.*, vol. 9, no. 8, 2010.

[12] L. Li, "Study on Security Architecture in the Internet of Things," in *Intemational Conference on Measurement, Information and Control (MIC) Study*, 2012, no. Mic, pp. 374–377.

[13] N. Using and E. Curves, "A Secured Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography," *Sensors*, pp. 4767–4779, 2011.

[14] M. Alizadeh, M. Salleh, M. Zamani, J. Shayan, and K. SASAN, "Security and Performance Evaluation of Lightweight Cryptographic Algorithms in RFID," *Recent Res. Commun. Comput.*, pp. 45–50, 2012.

[15] G. Avoine, M. A. Bingo, X. Carpent, S. Berna, O. Yalcin, and S. Member, "Privacy-Friendly Authentication in RFID Systems : On Sublinear Protocols Based on Symmetric-Key Cryptography," *EEE Trans. Mob. Comput.*, vol. 12, no. 10, pp. 2037–2049, 2013.

[16] D. Migault, D. Palomares, E. Herbert, W. You, G. Ganne, G. Arfaoui, and M. Laurent, "E2E : An Optimized IPsec Architecture for Secure And Fast Offload," in *Seventh International Conference on Availability, Reliability and Security E2E:*, 2012.

[17] E. Vasilomanolakis, J. Daubert, and M. Luthra, "On the Security and Privacy of Internet of Things Architectures and Systems," *darmstad Univ. J.*, 2015.

[18] B. Y. Mo, T. H. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "Cyber – Physical Security of a Smart Grid Infrastructure," *Proc. IEEE*, vol. 100, no. 1, pp. 195–209, 2012.

[19] B. S. Thakur and S. Chaudhary, "Content Sniffing Attack Detection in Client and Server Side : A Survey," *Int. J. Adv. Comput. Res.*, no. 2, pp. 4–7, 2013.

[20] S. Issues, "A Survey of RFID Deployment and Security Issues | Korea Science A Survey of RFID Deployment and Security Issues A Survey of RFID Deployment and Security Issues | Korea Science," *J. Inf. Process. Syst.*, vol. 7, no. 4, pp. 16–17, 2011.

[21] R. Uttarkar and P. R. Kulkarni, "Internet of Things : Architecture and Security," *Int. J. Comput. Appl.*, vol. 3, no. 4, pp. 12–19, 2014.

[22] V. Soni, P. Modi, and V. Chaudhri, "Detecting Sinkhole Attack in Wireless Sensor Network," *Int. J. Appl. or Innov. Eng. Manag.*, vol. 2, no. 2, pp. 29–32, 2013.

[23] R. P. Padhy, "Cloud Computing : Security Issues and Research Challenges," vol. 1, no. 2, pp. 136–146, 2011.

[24] W. Chen, R. K. Guha, T. J. Kwon, J. Lee, and Y. Hsu, "A survey and challenges in routing and data dissemination in vehicular ad hoc networks," *Wirel. Commun. Mob. Comput.*, no. October 2009, pp. 787–795, 2011.

[25] F. Baccelli, A. El Gamal, and D. N. C. Tse, "Interference Networks With Point-to-Point Codes," *IEEE Trans. Inf. THEORY*, vol. 57, no. 5, pp. 2582–2596, 2011.

[26] Z. Xu, Y. Yin, and J. Wang, "A Density-based Energy-efficient Clustering Algorithm for Wireless Sensor Networks," *Int. J. Futur. Gener. Commun. Netw.*, vol. 6, no. 1, pp. 75–86, 2013.

[27] S. Sharmila, "Detection of sinkhole Attack in Wireless Sensor Networks using Message Digest Algorithms," *IEEE*, pp. 0–5, 2011.

[28] S. Daneshmand, A. Jafarnia-jahromi, A. Broumandan, and G. Lachapelle, "A Low-Complexity GPS Anti-Spoofing Method Using a Multi-Antenna Array," *ION GNSS12 Conf.*, pp. 1–11, 2012.

[29] C. Chen, Y. Lin, Y. Lin, and H. Sun, "RCDA : Recoverable Concealed Data Aggregation for Data Integrity in Wireless Sensor Networks," *IEEE Trans. PARALLEL Distrib. Syst.*, vol. 23, no. 4, pp. 727–734, 2012.

[30] A. Razzaq, K. Latif, H. F. Ahmad, A. Hur, Z. Anwar, and P. C. Bloodsworth, "Semantic security against web application attacks," *Inf. Sci. (Ny).*, vol. 254, pp. 19–38, 2014.

[31] D. H. Patil, "Data Security over Cloud," *Int. J. Comput. Appl.*, pp. 11–14, 2012.

[32] B. R. Chandramouli and P. Mell, "State of Security Readiness," *Crossroads*, vol. 16, no. 3, pp. 23–25, 2010.

[33] K. Hashizume, D. G. Rosado, E. Fernández-medina, and E. B. Fernandez, "An analysis of security issues for cloud computing," pp. 1–13, 2013.

[34] N. Kilari and C. Applications, "A Survey on Security Threats for Cloud Computing," *Int. J. Eng. Res. Technol.*, vol. 1, no. 7, pp. 1–10, 2012.

[35] K. Dahbur, "A Survey of Risks , Threats and Vulnerabilities in Cloud Computing," in *International Conference on Intelligent Semantic Web-Services and Applications*, 2011.

[36] Y. Singh, F. Kandah, and W. Zhang, "A Secured Cost-effective Multi-Cloud Storage in Cloud Computing," *IEEE INFOCOM*, pp. 619–624, 2011.

[37] Z. Brakerski and V. Vaikuntanathan, "Efficient fully homomorphic encryption from (standard) LWE," *SIAM J. Comput.*, vol. 43.2, pp. 831–871, 2014.

[38] B. L. Suto, "Analyzing the Accuracy and Time Costs of Web Application Security Scanners," *San Fr.*, no. October 2007, 2010.

[39] S. Kumar, S. Pal, A. Kumar, and J. Ali, "Virtualization , The Great Thing and Issues in Cloud Computing," *Int. J. Curr. Eng. Technol.*, pp. 338–341, 2013.

[40] D. Koo, J. Hur, and H. Yoon, "Secure and efficient data retrieval over encrypted data using attribute-based encryption in cloud storage q," *Comput. Electr. Eng.*, vol. 39, no. 1, pp. 34–46, 2013.

[41] A. Tewari, A. K. Jain, and B. B. Gupta, "Recent survey of various defense mechanisms against phishing attacks," *J. Inf. Priv. Secur. ISSN*, vol. 6548, no. Feb, pp. 3–13, 2016.

[42] J. Wan, N. Cn, and A. No, "Malware detection using pattern classification," 2012.

[43] H. Tobias and E. Al., "Security Challenges in the IP-based Internet of Things," 2011.

[44] M. C. M and A. Serbanati, "An overview of privacy and security issues in the internet of things," *Springer*, 2010.

[45] A. Viejo, "Systems and methods for reducing unauthorized data recovery from solid-state storage devices," *Merry, Jr. al*, vol. 2, no. 12, p. Merry, Jr. et al, 2011.

[46] Y. Shin, A. Meneely, L. Williams, and J. A. Osborne, "Evaluating Complexity , Code Churn , and Developer Activity Metrics as Indicators of Software Vulnerabilities," *IEEE Trans. Softw. Eng.*, vol. 37, no. 6, pp. 772–787, 2011.

[47] W. Enck, D. Octeau, and P. Mcdaniel, "A Study of Android Application Security," *Syst. NTERNET NFRASTRUCTURE Secur.*, no. August, 2011.

[48] D. William, W. Surrey, and J. F. Benedict, "Authentication using application authentication element," 2012.

[49] M. Ongtang, S. Mclaughlin, W. Enck, and P. Mcdaniel, "Semantically rich application-centric security in Android," *Secur. Commun. Networks*, no. August 2011, pp. 658–673, 2012.

[50] S. L. Wiley, O. Park, and U. S. C, "Pin-hole firewall for communicating data packets on a packet network," 2011.

[51] C. Liu and Y. Zhang, "Research on Dynamical Security Risk Assessment for the Internet of Things Inspired by Immunology," in *8th International Conference on Natural Computation*, 2012, no. Icnc, pp. 874–878.