Application of Fog Computing in Military Operations

Divya Lanka
Assistant Professor, CSE
Vishnu Institute of Technology
Bhimavaram

Ch. Lakshmi Veenadhari
Assistant Professor, CSE
Vishnu Institute of Technology
Bhimavaram

D. Suryanarayana
Professor, CSE
Vishnu Institute of Technology
Bhimavaram

ABSTRACT
This paper clearly explains about the integration of fog computing in cloud environment to implement in military operation based applications. It explains the working model with fog computing. This approach is purely an outcome of the advantages of fog computing over the breaches with cloud computing. Thus, this will be a solution in most of the applications by including this technology in wireless sensor networks. This architecture was developed for providing high end secure applications. This approach has been applied to overcome the vulnerabilities in the real time applications using wireless sensor networks. This approach is performed in military applications to take spontaneous decision making by the military officials. Therefore this paper presents the reliable model in many smart wireless sensor networks.

General Terms
Edge Computing, Internet of Things, Pervasive Computing.

Keywords
Fog Computing, Cloud Computing, Military Applications, Smart Wireless Sensor Networks.

1. INTRODUCTION
The purpose of the work is to enhance the usage of fog computing as internet of things is playing a major role in every one's day to day life. From a farmer to a business man internet is a vital essential and most of the things relay on the internet. Wireless sensor network can be used in military environment to safeguard the motherlands to decrease the valuable deaths of the soldiers. In view of the fact that when using classical cloud computing in such scenarios, the limitations like response time, computational latency and data dissemination time may not be apt for such timely conditions. So, to take decisions fast to decrease response time and latency cloud can be replaced by fog computing providing more security because of sensitive data. The significance of this study is to highlight the features of fog computing which is a subset of the cloud. The interconnections between fog nodes and clouds are shown in the Figure1.

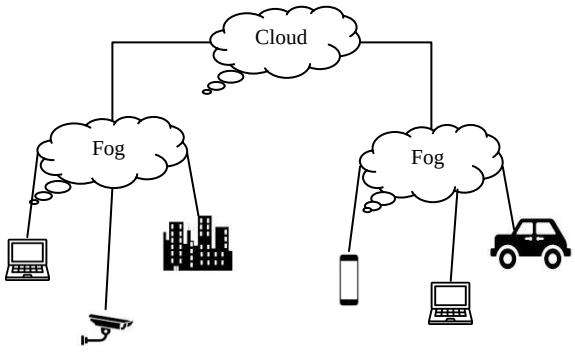

Fig 1: Design of Fog and Cloud Computing

Traditionally, the usage of Internet is very less and the amount of data is also limited because of the high cost of the internet, bandwidth and the resources. Later due to the fall in the cost of internet charges and development of wide variety of devices, new technologies, world widely the manual work is replaced by automotive work by the help of computers and other devices. All the information is stored in the cloud and applications run on the cloud to give the result to the end users. Not restricted to particular area, the usage of internet is out of bounds at present due to immense raise in wide variety of mobile and smart devices. Internet plays a major role in our day to day activities. With the miniature devices and convenience dependency on the internet is increasing along with that, load on the internet servers is also increasing which led to the evolution of fog computing. The information is stored in the fog locally and many applications run on the fog to give the result to the edge devices as shown in Figure 2. This is also reserved as EDGE Computing. The data is maintained centrally at remote servers, managed, and backed up. Cloud allows the users to store files online, so that they can access them from any location through the Internet. Hoang T. Dinh et.al, proposed a survey on mobile cloud computing applications and architecture [1].

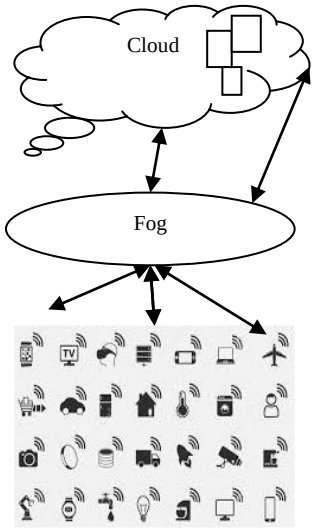

Fig 2: Fog and Cloud nodes in IOT

2. DISSIMILARITIES BETWEEN CLOUD COMPUTING AND FOG COMPUTING
The major variation between cloud computing and fog computing is how close the services are to the end users that is geographic spatial separation [2]. CISCO proposed fog computing to run multiple applications directly on billions of heterogeneous connected devices at the edges of network

through the Internet of Things (IoT) [3]. Customers can develop, manage and run software applications on Cisco IOx framework enables users to develop, manage, run software applications on networked devices like routers, switches and IP video cameras. Cisco IOx brings the Linux as open source software and Cisco IOS network operating system together in a solo networked machine (initially in routers). The variation of cloud computing and fog computing is shown in table1.

2.1 Overview of Fog Computing

Behind the advantages of the cloud like flexibility, disaster recovery, automatic software updates, Work from anywhere, improved collaboration, Security, Environmentally friendly still it have limitations like it requires lots of bandwidth, security, integrity, computational efficiency, storage efficiency, communication efficiency. Faheem Zafar et.al, presented data integrity polices for outgoing data and security challenges that come across with cloud storage and highlights the importance of data integrity schemes for outsourced data[4]. Diogo A. B. Fernandes et.al., proposed the vulnerabilities, threats, attacks on the cloud as cloud was being extensively used in various organizations[5]. Aepona describes Mobile Cloud Computing as a new concept for mobile applications by storing the data and processing of information are done at computing platforms rather than at mobile devices. [6]. Wireless networks have limitations like power consumption, lack of mobility support and location-awareness. By Fog, the amount of bandwidth needed is greatly reduced. Data processing and applications are concreted in the cloud. As, the mobile devices exploded in number producing huge amounts of data increasing the latency at the devices. To decrease such latency the applications should be processed at the device itself on the fog nodes. Data would not need to be transmitted using cloud computing networks since all of that is kept on smart devices. Fog bypasses through the internet, keeping data as local as possible. Most valuable data may be transmitted through cloud networks, but much of the traffic would kept away of the networks letting bandwidth free for everyone using cloud. Any node with computing, storage and network connectivity can be a fog node. The fog applications are very diverse in nature.

As the load on the cloud was increasing day by day, there are still odd issues odd due to inherent problems of cloud computing such as unreliable latency, lack of mobility support and location-awareness. Fog computing addresses the problems of cloud by providing flexible resources and services to end users at the edges of network, while cloud computing provides resources in the mainstay network [7].

Amazon Elastic Compute Cloud (Amazon EC2) is a web service that is secure, variable size, cost effective, reliable, robust, scalable, fault tolerant, and eases of computing for developers compute capacity in the cloud. This simple web service gives full control over the users computing resources and allows running on Amazon's proven computing environment. Amazon EC2 allows the customers to pay only for the cloud capacity they actually used [8]. Amazon web services developed a fog for community contributed software that helps its customers to use low level API calls for using data that is frequently used and hides the unused data in cloud that supports various cloud providers and services in a clean, robust and consistent fashion.

Google providing Google cloud platform for secure, global, high performance, attractive cost and also provides powerful analytics on big data to give fast answers. Fog provides server less capabilities, low latency access to media as pervasive computing and real time data synchronization across all mobile platforms.

Table 1. Dissimilarities between cloud computing and fog computing

Constraints	Cloud Computing	Fog Computing
Geographic occupancy	Centralized	Decentralized
Awareness of location	No awareness	Possible
Connectivity	Dedicated Leased Line	Wireless
Computing	Centralized at servers	Ubiquitous
Possibility of Attacks	More prone to attacks	Less prone to attacks
Server Nodes	Limited number of servers	Many nodes act as server nodes
Latency	High	Low
Bandwidth	Requires High Bandwidth	Requires Less Bandwidth
Mobility	Limited Mobility	More mobility is there
Hops to Travel	Should Travel Multiple Hops	Should Travel Single Hop
Transmission Delay	High Delay is there	Low Delay is there
Processing Speed	More time to process information	Less Time to process information
Fault Tolerance	YES	YES

2.2 Security Features in Fog Computing

Security in cloud is a major problem in cloud computing as it provides storage space for users to save their information and retrieve their information using third party data centre's. Mainly two security issues in cloud computing: security issues faced by cloud providers and their customers. The cloud providers ensure that their infrastructure is secure to protect the clients data and applications. Data would not need to be transmitted using cloud computing networks since all of that is kept on smart devices by pass through the internet, keeping it as local as possible. Most valuable data may still be transmitted through cloud networks, but much of the traffic would be kept off of those networks. Ivan Stojmenovic et.al, studied man-in-the-middle attack in Fog computing and stealthy features of this attack by observing Processor and memory consumption on Fog device [9]. Also discussed authentication and authorization techniques that can be implemented in Fog computing. Fog environment is being protected by using decoy systems to detect and intimate either visually and audibly regarding the unauthorized data access to the owner of the data.

3. WIRELESS SENSOR NETWORKS

A network can be infrastructure dependent, devices depend on base stations and access points as shown in Figure 3. A sensor is a electronic device that senses its surroundings and sends information to a centralized device like a computer. Traditionally, a sensor is used to detect only temperature, pressure and flow. But, currently sensors not only sensing data but also having features like data processing and less distance communication. Because of their additional features like low cost, portable size, less power consumption the sensor nodes has grown enormously.

Connecting a group of sensor nodes forms a network called sensor network and they operate in wireless manner with unguided media that is which is called Wireless Sensor Network. Routing plays a major role in wireless sensor networks there are many routing, power management, and data broadcasting protocols were specially designed for energy harvesting in WSNs. Routing protocols in WSNs might differ depending on the application and network architecture. Overall, the routing techniques are classified into three categories depending on the structure of the primary network: flit, hierarchical, and location-based routing. Furthermore, these protocols can be classified into multipath-based, query-based, negotiation-based, QoS-based, and coherent-based depending on the protocol operation [10]. Due to the development of (mems) Micro electro mechanical systems technology, wireless Communications and digital electronics there was a vast coverage of wireless sensor networks in any point of the world from the remote areas to the highly populated areas[11].

Now a day's wireless sensor networks are being used in manufacturing, Industries electronic devices, airplanes and aerospace, automobiles, hospitals for medical treatment, robotics and many other aspects of our day-to-day life. A good sensor is sensitive to the measured property, insensitive to any other property not defined in its application, and should not show impact on the measured property. There are various sensors like chemical sensors, biosensors, image sensors. Wireless Sensor Networks (WSN) is a pervasive computing environment used on a large scale to monitor real-time environmental status [12]. A number of parameters required by the target application, which includes range, antenna type, target technology, components, memory, storage, power, life time, security, computational capability, communication technology, power, size, programming interface.

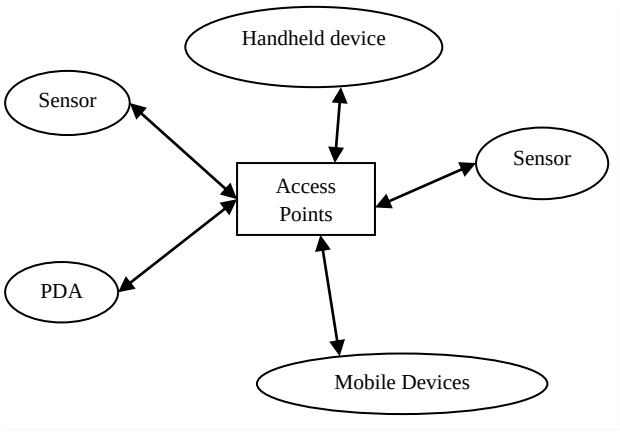

Fig 3: Infrastructure Dependent Network

These applications should be considered while designing a wireless sensor node [13]. A. Flammini et.al., proposed that Wireless Sensor Network is one kind of Internet of things that uses cloud computing services to optimize information management, sharing monitored values and improving QOS[14]. According to NIST, Cloud Computing (CC) is an technology that provides convenient, on-demand network access to a shared pool of configurable computing resources that is robust and unconfined with less management effort[15]. Werner kurshl et.al presented a model that aggregates wireless sensor networks with the cloud computing environment and the useful nature of such aggregation [16]. Samia Bouzefrane introduced the service architecture towards the applications of mobile devices, sensors and cloud computing [17]. Wireless Sensor Network is a special kind of mobile adhoc network as in Figure 4. that does not rely on base transceiver stations and access points. With the development of wireless communication and intelligent computation, sensor nodes has become smart sensors which are capable of not only observing physical parameters around surroundings but also capable to process, communicate, compute and network the sensed information. After data aggregation, data compaction and Data Fusion only the data is dispersed. Wireless sensor networks can be used in wide variety of areas like military, street lighting, traffic monitoring, medical applications, home automation, environmental monitoring and etc.

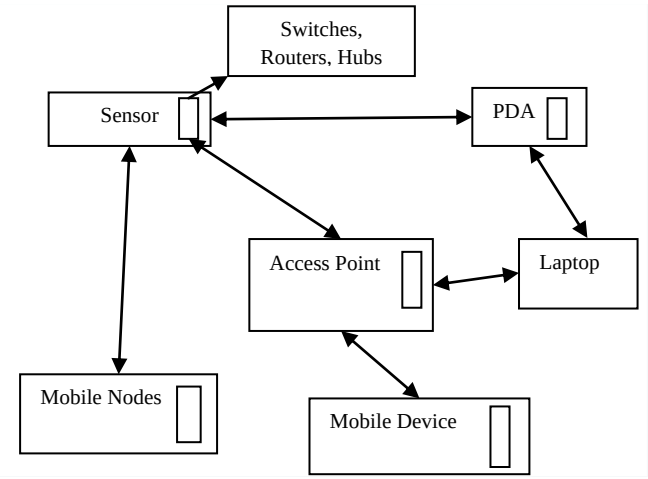

Fig 4: Infrastructure Independent Network

4. IMPLEMENTATION

The proposed system can be implemented in One real time Scenario of wireless sensor networks in military applications, border security and prisons. The border was secretly monitored by agents hired, building miles of fences, deploying cameras at the fences, etc. Along with these services wireless sensor networks can also be used to enhance the security at the borders. On September 18th 2016 four militants had attacked the Indian army at Uri Indian-administered state of Jammu and Kashmir, and killed 19 soldiers. After the attack on Uri army base security forces like Border Security Force (BSF) and the army paid complete alert along the 198-km long international border (IB) and 744-km long Line of Control (LoC). To control the attacks at the borders smart wireless sensor networks along fog computing can be proposed to take action in less time as in Figure 5.

Fig 5: Manual Tracking Replaced with Sensors

DAI Hong-yang et al, proposed that due to the development in electronic and computer technology's wireless sensor network is extensively applied in military field application and the advantages of using wireless sensor networks[18]. Boselin Prabhu et.al, proposed the use of wireless sensor networks in military applications to improve the troop

readiness and decrease the reaction time and tactical planning for deploying troops effectively can be done [19]. The implementation should be fault tolerant if any one node fails it should not ruin the whole network. Fault tolerance plays a crucial role in wireless sensor networks even when some components fail, network continues to operate properly. With the sensor node characteristics, radio communications and unfriendly environments these networks are deployed. The WSN mechanisms fault tolerance property of wireless sensor networks include prevention of fault occurrence such as power aware routing, data aggregation and compression. Depending on size in terms of covered geographical area and number of nodes the mechanisms can be chosen. Protocols for small networks are poor for large networks and vice versa.[24]. Đurišić, M. P., Tafa et.al, discussed sensor networks in Defense related applications, various sensor types and their capabilities and determined the usage of WSNs.[25]

5. DESIGN

A three tier architecture is proposed for military applications like sensor nodes in tier-1 connected to fog nodes in tier-2 and data can be communicated from fog nodes to cloud nodes on timely basis as shown in Figure 6.

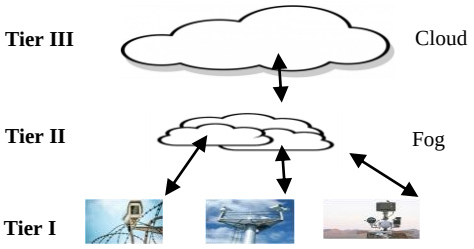

Fig 6: Three Tier Architecture

5.1 Requirements for the proposed system

The below are some of the requirements needed for our proposed model to maintain the system in accurate and reliable.

- Data should be maintained spontaneously when needed
- Resistant to fault tolerance, direction finding and other electronic warfare threats
- Maintaining data security at the data centre (the cloud) and at the edge devices
- Sensors can be deployed in the war field by motor vehicles, by personal or backpack of army men. For this reason sensors must be weight less and miniature
- As sensors are a type of Adhoc networks they should have properties to reconfigure themselves by identifying neighbour nodes within its transmission range
- Sensor should operate in full duplex mode for efficient communication
- As sensors are battery dependent, energy harvesting algorithms must be used to increase life of a sensor node
- Data sensed by the nodes should be reliable so that the commandants take spot decisions

5.2 Security Measures to be taken

Security issues like IP Spoofing, Denial of service, man in the middle attack, confidentiality, eaves dropping, atomic transfer of data, non repudiation and consistency should overcome by applying proper security features in the system.

Traditionally the main problem with cloud is its security, to enhance the security features of cloud computing, fog computing has come into existence. At present, decoy systems are being used in fog computing to overcome the breaches in cloud computing. As the fog node bypasses the cloud, fog node gets encrypted data from cloud, even encrypted can be stolen by man in the middle attacks. To overcome that encryption of data can be done at fog node as well by using advanced encryption standard (AES) algorithm. Encrypting the beforehand encrypted data is more secure and defends against the attacker more accurately provides better security in the fog computing to handle sensitive data [20]. The proper use of decoy system is valuable than Intrusion detection system. Decoy technology like honey pots, honey files, bogus information that secure data against the internal attacks at cloud provider. Monitoring the abnormalities in data access patterns helps to find the intruders. When situations arise the user can be verified with many challenging questions to protect over misuse of real users data. Deploying the decoy information at Cloud service customer in the cloud and by the individual users in their private social network profiles can offense data attacks on cloud [21]. If any unauthorized access is suspected they are verified using challenge questions and disinformation attack by disseminating large amounts of decoy information to the intruder [22].

5.3 Flow Chart

To achieve the goals of potency, efficacy and security U.S. Department of Defense has mandated that its networks be consolidated and view of military networks as an enterprise. Consolidation efforts are effective in permanent, garrison networks that are connected with high bandwidth, fiber optic cables. On Implementation of critical services and data in the cloud saves resources and increase cyber security. Considering military as an enterprise stores all data in the cloud[23]. The flow of the proposed system by introducing fog computing is that at first, the system is initialized. Which mean that the sensor nodes are to be deployed by hand or backpack of soldiers or by vehicles. Then the nodes have to locate the neighboring nodes within their transmission range and organize themselves into a network as wireless sensor network is a variation of adhoc network. Once forming a network they senses their surroundings for the invaders. If the sensors sensed any then the distance is measured. Suppose the distance is within the bounds then the information if passed to the fog node and sends information to the proper personnel. Timely the data from fog nodes is sent to the cloud as the fog nodes has limited memory to store. Incorporating applications like gait recognition technology with our proposed system may helpful to provide a strong and secure system [26]. Likewise the system can be injected to military and border security to enhance the security features of the army forces. The flowchart is shown in Figure 7.

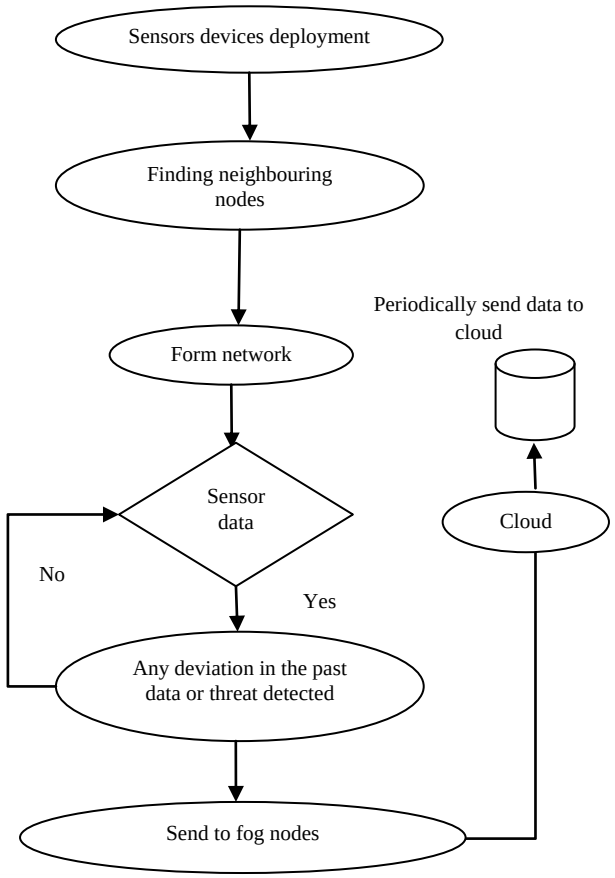

Fig 7: Flow chart for the implementation

6. CONCLUSION

Implementing fog computing on such an adhoc networks help to take decisions spontaneously as early detection could make situations better and the military official's can plan accordingly with the sensed data. Usage of fog computing decreases the latency, power consumption, storage when compared to cloud computing, where in the military field, time and action take a prominent role. By the use of fog computing boarder security can be enhanced as a smart security.

In future work this system can be implemented in hardware and can be applied to many real time environments for the public security by the government bodies to safeguard their motherlands from the hands of the enemy troops.Fog Computing moves the task of data center's to the edge of the network with minimum latency, less computing and networking services in a decentralized way. This type of computing can be used in health care applications and in many real time Internet of Things applications like visual security and smart cities.

7. ACKNOWLEDGMENTS

Our thanks to Mr. S. Mahaboob Hussain, Coordinator Research, Vishnu Institute of Technology and Ms. Prathyusha Kanakam, MVGRCE, for their inputs towards this research work.

8. REFERENCES

[1] Dinh, H. T., Lee, C., Niyato, D., & Wang, P. (2013). A survey of mobile cloud computing: architecture, applications, and approaches. Wireless communications and mobile computing, 13(18), 1587-1611.

[2] Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012, August). Fog computing and its role in the internet of things. In Proceedings of the first edition of the MCC workshop on Mobile cloud computing (pp. 13-16). ACM.

[3] Bonomi, F. (2011, September). Connected vehicles, the internet of things, and fog computing. In The Eighth ACM International Workshop on Vehicular Inter-Networking (VANET), Las Vegas, USA (pp. 13-15).

[4] Zafar, F., Khan, A., Malik, S. U. R., Ahmed, M., Anjum, A., Khan, M. I., ... & Jamil, F. (2017). A survey of cloud computing data integrity schemes: Design challenges, taxonomy and future trends. Computers & Security, 65, 29-49.

[5] Fernandes, D. A., Soares, L. F., Gomes, J. V., Freire, M. M., & Inácio, P. R. (2014). Security issues in cloud environments: a survey. International Journal of Information Security, 13(2), 113-170.

[6] White Paper. Mobile Cloud Computing Solution Brief.AEPONA, 2010.

[7] Yi, S., Li, C., & Li, Q. (2015, June). A survey of fog computing: concepts, applications and issues. In Proceedings of the 2015 Workshop on Mobile Big Data (pp. 37-42). ACM.

[8] Elastic Compute Cloud (EC2) – Cloud Server & Hosting – AWS. (2017). Amazon Web Services, Inc.. Retrieved 6 February 2017, from https://aws.amazon.com/ec2/

[9] Stojmenovic, I., Wen, S., Huang, X., & Luan, H. (2015). An overview of Fog computing and its security issues. Concurrency and Computation: Practice and Experience.

[10] Al-Karaki, J. N., & Kamal, A. E. (2004). Routing techniques in wireless sensor networks: a survey. IEEE wireless communications, 11(6), 6-28.

[11] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). Wireless sensor networks: a survey. Computer networks, 38(4), 393-422.

[12] Kanakam, P., Hussain, S. M., & Chakravarthy, A. S. N. (2015, December). Electronic noses: Forestalling fire disasters: A technique to prevent false fire alarms and fatal casualties. In Computational Intelligence and Computing Research (ICCIC), 2015 IEEE International Conference on (pp. 1-6). IEEE.

[13] Potdar, V., Sharif, A., & Chang, E. (2009, May). Wireless sensor networks: A survey. In Advanced Information Networking and Applications Workshops, 2009. WAINA'09. International Conference on (pp. 636-641). IEEE.

[14] Flammini, A., & Sisinni, E. (2014). Wireless sensor networking in the Internet of Things and cloud computing era. Procedia Engineering, 87, 672-679.

[15] Benefits of Cloud computing To Wireless Sensor Networks – Wireless Sensor Networks Magazine.

(2017). Wsnmagazine.com. Retrieved 16 March 2017, from https://www.wsnmagazine.com/cloud-computing-wsn/

[16] Kurschl, W., & Beer, W. (2009, December). Combining cloud computing and wireless sensor networks. In Proceedings of the 11th International Conference on Information Integration and Web-based Applications & Services (pp. 512-518). ACM.

[17] Le Vinh, T., Bouzefrane, S., Farinone, J. M., Attar, A., & Kennedy, B. P. (2015). Middleware to integrate mobile devices, sensors and cloud computing. Procedia Computer Science, 52, 234-243.

[18] DAI, H. Y., TANG, H., & HU, X. P. (2010). Wireless Sensor Networks in Military Application. Computer Knowledge and Technology, 16, 034.

[19] Prabhu, B., Pradeep, M., & Gajendran, E. (2017). Military Applications of Wireless Sensor Network System.

[20] Vishwanath, A., Peruri, R., & He, J. S. (2016). Security in fog computing through encryption. International Journal of Information Technology and Computer Science (IJITCS), 8(5), 28.

[21] KAREKAR, S. P., & VAIDYA, S. M. (2015). Perspective of Decoy Technique using Mobile Fog Computing with Effect to Wireless Environment.

[22] Stolfo, S. J., Salem, M. B., & Keromytis, A. D. (2012, May). Fog computing: Mitigating insider data theft attacks in the cloud. In Security and Privacy Workshops (SPW), 2012 IEEE Symposium on (pp. 125-128). IEEE.

[23] Powell Jr, D. A. (2013). The Military Applications of Cloud Computing Technologies. ARMY COMMAND AND GENERAL STAFF COLLEGE FORT LEAVENWORTH KS SCHOOL OF ADVANCED MILITARY STUDIES.

[24] Chouikhi, S., El Korbi, I., Ghamri-Doudane, Y., & Saidane, L. A. (2015). A survey on fault tolerance in small and large scale wireless sensor networks. Computer Communications, 69, 22-37.

[25] Đurišić, M. P., Tafa, Z., Dimić, G., & Milutinović, V. (2012, June). A survey of military applications of wireless sensor networks. In Embedded Computing (MECO), 2012 Mediterranean Conference on (pp. 196-199). IEEE

[26] K. Prathyusha, S. M. Hussain and A. S. N. Chakravarthy, "A cognitive perceptive framework with gait recognition technology," 2016 2nd International Conference on Next Generation Computing Technologies (NGCT), Dehradun, India, 2016, pp. 665-669.