Internet of Things : Vehicular Clouds

By Group 16 : Ruifeng Luo, Wuang Shen, Tiange Wang

1. Abstract

Since around the late 1990s, the growing trend of electronic devices has been taken place in our modern society. Electronic devices are designed to enhance efficiency at work and make our life easier, especially for devices connecting to the internet of things(IoT). Among those technologies, the self-driving car is the most advanced. According to the statistics from the researcher (Fast Company, 2017), the crash rate of the self-driving car,3.2 accidents/million miles is much better than the national crash rate,4.2 accidents/million miles. However, the most advanced technology may have potential security threats over vehicular clouds.

In this report, the vehicular clouds and its key components are discussed. This paper will also explain how each key component related to vehicular clouds. And the analysis will provide the insights to security challenges as the number of the self-driving car increased in our modern society. Those challenges will be analyzed throughout following parts: confidentiality, authentication, integrity. Additionally, the cryptographic algorithms like Data Encryption Standard(DES), Advanced Encryption Standard(AES) and Rivest-Shamir-Adleman(RSA) Will be explored since it may affect the performance of cloud computing based on its security level.

2. Introduction

Internet of things is becoming the most important concept in our both workplace and somewhere else. It is a system interconnecting with electronic devices and anything that can be connected with networks. Internet of things provides ability to transfer information over the network without objects interaction such as people, computing devices.

Many modern vehicles equipped with advanced networking and communicating devices have the capability of sending and receiving processed data and communicating with external devices over network protocols (He, W., Yan, G. and Xu, L,2014). Cloud computing allows autonomous vehicles to retrieve information on other vehicles on the same network. It provides a modern way of solving numerous issues in our society, such as Traffic congestion and road safety.

Although cloud computing and internet of things(IoT) provide a modern way of improving our daily life, there still exists security threats to be considered in the vehicular clouds. In this report, we discuss key components from vehicular clouds. We also provide the analysis to it throughout several potential security threats and corresponding algorithms.

3. Applications and cloud related to IoT

Vehicular cloud

Vehicular cloud allows self-driving vehicles to perform as an intelligent agent, which provides better vehicle-to-vehicle communication on the cloud. It addresses numerous transportation issues. In this section, the functionality of vehicular clouds such as corresponding platform, networks and computing, are described.

3.1 Vehicular Cloud Computing

In the local area, the vehicular cloud allows several vehicles to communicate to each other continuously, and the individual can store/downloading information from the internet. If one node is detected as a suspicious node, the other receiving node are trying to avoid receiving data from the node. For example, from figure 1, the transmit node notifies those receiving nodes in the local area since transmit node has detected the blocking caused by accidents. Receiving nodes could efficiently to avoid the accident blocking.

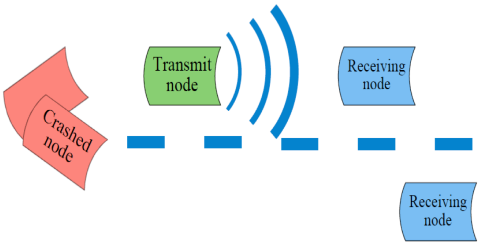

Figure (1). Accidents blocking
Note. From ‘CyberSecurity Considerations for an Interconnected Self-Driving Car System of Systems ‘(Jeremy, S., John, M., Brett Y, Mitchell, S., Abdullah, A., Kelvin, B., and Jordan, Hartman.)

Furthermore, combining the vehicular cloud platform with IoT and various electronic devices creates vehicle-to-vehicle communication mechanisms and enable vehicles to retrieve and exchange data between devices such as vehicles, roadside cameras and streetlights. From figure 2, the cloud platform provides services to customers through the conventional cloud and temporary cloud. Temporary cloud supports dynamic vehicular applications, and it is designed to make compatible of the conventional cloud to vehicles increasing capabilities of data storage, processing and computing. However, most applications on the temporary cloud have issues running on conventional cloud. And often, the temporary cloud is required to make the exchange of data from the conventional cloud and share resources on the cloud platform. Hence, the compound of following services is used to solve this problem. Both types of cloud support on the following cloud services (He, W., Yan, G. and Xu, L,2014).

- Storage as a service(SaaS)
  For applications, they may need a large amount of storage space. In this case, each vehicle shares their unused storage space as cloud-based storage service.
- Platform as a service(PAAS)
  Vehicular cloud provides some assistant services such as black spot location warning, parking availability and lane change warning.
- Network and data processing as a service (IAAS)
  Vehicle cloud provides its capabilities of networking and data processing to other vehicles throughout the cloud so that multiple vehicles can work on the same task, which indicates less time-consuming.

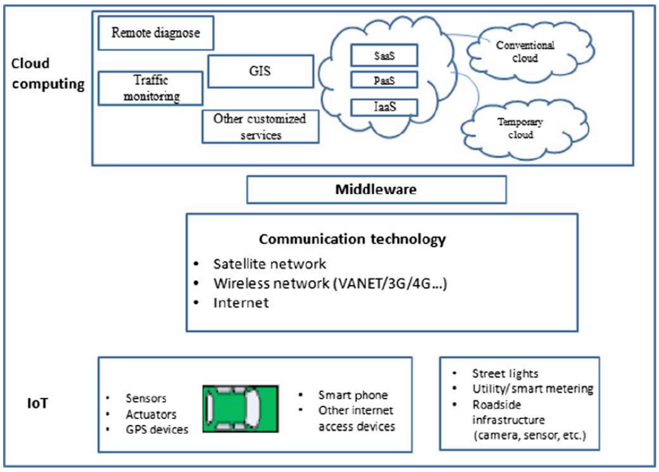

Figure (2). Architecture for vehicular data cloud
Note. From ‘Developing Vehicular Data Cloud Services in the IoT Environment' (He, W., Yan, G. and Xu, L, 2014)

3.2 Information Centric Networking

As Mario, G., Eun-Kyu, L., Giovanni, P, and Uichin L. (2014) states that Information Centric Networking ICN is a general model of communication architecture. And the goal of ICN is to distributing contents over internet efficiently. According to figure 3, ICN is the emphasis on what contents are and how to distribute over the internet, other than where the contents come from. The publisher publishes the contents on the internet so that consumers can retrieve contents on the internet by sending requests.

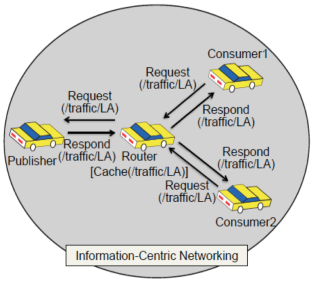

Figure (3). Information Centric Networking
Note. From ‘Internet of Vehicles: From Intelligent Grid to Autonomous Cars and Vehicular Clouds‘(Mario, G., Eun-Kyu, L., Giovanni, P, and Uichin L,2014)

3.2 Cloud Resources

The vehicular cloud can be distinguished from the internet cloud since vehicular cloud is created temporarily by interconnected resources in the local area and roadside units such as cameras and street lights. And the vehicular cloud is created to provide the cooperation among those objects (e.g.

vehicles, cameras and streetlights) in the local area. It also provides services that each vehicle cannot produce. Vehicular cloud computing, along with information centric network, is joined together to create virtual cloud platform and distribute contents more efficient.

The resources are categorized into three components: sensing resource, computing resource and data storage resource. Data storage resource is considered to be the storage that stores content from any applications, sensing and multiple media. That contents stored in the storage shared among those vehicles in the local area to provide services such as, searching query and responding with relevant information. Sensing resource are referred to the ability of sensor that detect the particular events in the effective area. Each sensor connects to the internet and cloud so that the sensing resources are sharing on the virtual platform and linked to the external systems.

As we can see from figure 4, all the resources, computing, sensing and data storage resources, are shared over cloud by creating the common virtual platform so that vehicle-to-vehicle communications run efficiently.

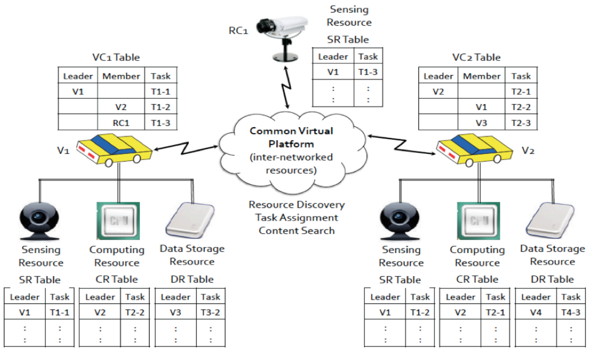

Figure (4). Cloud resources 1
Note. From 'Internet of Vehicles: From Intelligent Grid to Autonomous Cars and Vehicular Clouds' (Mario, G., Eun-Kyu, L., Giovanni, P, and Uichin L,2014)

From the figure 5,

- Suppose the V1 is the cloud leader that create vehicular cloud computing service and provide it to self-driving vehicle application. Since the V1 have only one image of the road segments, and it requires the images of other road segments to accurate the current contents, V1 sends out a message(RREQ) to find objects (vehicles and roadside units) in that local area which can provide the resources.
- Then based on the replied message(RREP) from objects, the V1 forms a new cloud with selected new members (in this picture, the new members are V2 and RC1).
- Afterwards, V1 asks objects to get the pictures of other road segment images. Since V1 has collected all the images from other members, it creates new contents and publishes to the cloud network area. It asks another object (e.g. V4) to store in their storage space in case of reusing the contents in the future. When the other vehicles, V6 and V7, required particular contents over the cloud, they request contents with a message. Since there exist the contents in V4, V4 sends those contents to V6 and V7 directly.
- If V1 decides not to utilize the cloud, then it sends out release message over the cloud. In this case, RC1 and V2 received release message.

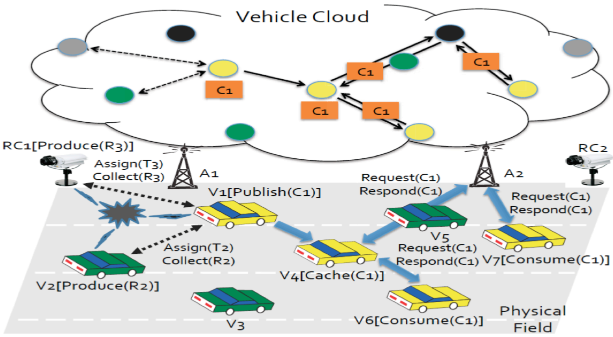

Figure (5). Cloud resources 2
Note. From 'Internet of Vehicles: From Intelligent Grid to Autonomous Cars and Vehicular Clouds'(Mario, G., Eun-Kyu, L., Giovanni, P, and Uichin L,2014)

4. Challenges and Attacks:

Same as other IoT components, security challenges are parts of main challenges faced by self-drive car based on Vehicular Cloud. Traditional cyber-attacks may leak data, modify messages, etc. but it never threatens humans' life directly. Different from traditional cyber security problems, criminal acts like exploiting the vulnerability of the system and applying cyber-attacks to a self-drive car will directly put user's life in danger. Greenberg (2015) demonstrates how dangerous the vehicular cyber security threats could be when ethical hackers take advantages of vulnerabilities of car's electronic control units and remotely control the car. Thus, it is necessary to be aware of some potential security challenges for self-drive car base on Vehicular Cloud, to guarantee the safety of self-drive vehicles. Security challenges like Confidentiality, Authentication, data integrity and other possible threats along with some potential attacks will be discussed in this section.

4.1 Confidentiality

Confidentiality of the system prevents other third parties to read transmit data. A massive amount of real time data will transfer between cloud and local car device. Those data gathering from sensors and other devices will contain some private information. For example, user's planned routes between starting point and destination. According to Mekki et al. (2016), vehicles' location and identity will be transmitted in vehicular communications. Those two privacy elements are essential parts that need to be protected to ensure the confidentiality of the system.

4.1.1 Location

To better assist the decision algorithm run on the cloud server, it is necessary that the local car can continuously update some location information to the cloud. Then based on the location that car provided, the cloud server can check the traffic condition of self-drive car's nearby roads. For example, by informed with car's location, the server can get information such as the weather, road accidents and traffic flow from other components of the system. The decision algorithm like machine learning algorithm will input those traffic condition data, to update the running path. However, without protection for data confidentiality, a black-hat attacker could take advantage of those disclosed private location information to implement their attacks. For example, attackers can use location information to predict user's personal information like their potential social activities and relations. Besides this also provide attacker sufficient information to plot criminal activities like physical attack, kidnap or even murder.

4.1.2 Identity

User's identity is bounded with self-drive vehicle's ID. To integrate the car with other services like Open Road Tolling (ORT), car's identity should link to owner's identity to provide user's personal information like credit card or insurance plan. Data transmission between vehicle and cloud or even Vehicle to Vehicle (V2V) will require an exchange of identities. Without a secured protocol, this process may disclose owner's identity to attackers. In this case, attackers are provided with an opportunity to utilise car's identity as a resource to plan some attacks. For example, owner's credit card information is highly likely to be obtained by attackers if they can provide user's ID and Car's ID. Thus, protecting user's identity is also an essential segment of the confidentiality of autonomous vehicles.

4.2 Authentication

The identity of vehicle and cloud provider needs to be verified to ensure the authentication of the system. Self-drives cars should be capable of travelling around different areas, so sometimes cars may need to switch the cloud provider to be able to process data. Without verifying the identity of the cloud provider or other vehicles during V2V communication, a self-drive car will be vulnerable to some attacks like man-in-middle attack. By applying this cyber-attack scheme, attackers can pretend to be A when they communicate with B and pretend to be B when they communicate with A, where both A and B may not notice that they are communicating with attackers rather than their targeted recipient. If attackers impersonate to be a cloud provider, they can manipulate transmitted data and send a list of malicious guide to the car or a list of fake car information to the cloud, then let the car running on the wrong path or even make car accidents happen. Furthermore, as Whaiduzzaman et al.(2013) discussed in their report, authenticating components in vehicular clouds environment is more challenging than other networks because vehicles will keep changing their locations. In this case, some authentication methods based on location information will fail to verify the identity of a vehicle, Besides, according to Yan et al. (2013), the recipient of authentication message may be out of valid range because of car's limited transmission range and high mobility. Those challenges make authentication methods less available to the autonomous car system and thus results in the system lower security level.

4.3 Data Integrity

Similar to authentication challenges, the system should be able to detect whether there exists unauthorised third party manipulated transmitted data or data loss in the transport layer. Either raw data from the car or guide from the cloud been manipulated will put user's life in danger. Moreover, due to noise or connection congestion in the transmission, data packets may have a high risk of losing data. For instance, if the system using User Datagram Protocol (UDP) in the transport layer, when a packet is sent out, it is hard to tell whether the message will reach the destination or not, then the data integrity will not be guaranteed in this situation. Apart from the data loss, connection loss is another factor may cause the system incomplete data integrity. The performance of Autonomous vehicles' will be highly related to the network connection to the cloud. The unstable network will cause time lag, which will make transferred data inaccurate and even lead it to safety issues. Although 5G network in future can provide a stable network environment for the self-drive car, connection loss is still possible when vehicles run in some rural areas where are not equipped with developed infrastructure.

4.4 Other Challenges

There are also some challenges faced by cloud provider but will also bring up security threats to an autonomous vehicle, like the cloud server may break down if it is getting some attacks like Denial of Service (DoS) attack. In this case, attackers will exploit the vulnerability in the cloud server and cause the server overloaded, which leads the server temporarily unavailable to cloud user. Affected by this attack, autonomous vehicles that totally depend on cloud service will be unable to operate, and users have to manually control cars instead. Some self-drive cars have an off-line system can deal with the situation when the vehicle lost the service from cloud providers, but it will still affect car's performance, because local devices may not be equipped with efficient processors or enough storages as what cloud servers have to process and store data.

5. Countermeasure and Discussion

In this section, solutions for threats, primary challenges and security problems will be demonstrated.

Three primary challenges were summarised in the previous section:

- **Data leakage**
- **Cloud provider's identity**
- **Information integrity**

5.1 **Data Leakage**

Data leakage refers to that when the self-driving car is driving on the way, and it is probable that hackers have opportunities to intrude the database and steal data during the transmission and exchange of data from the car to the cloud (Zhao and Ge, 2013). Hence, it is necessary to enhance the security level of communications. The AES (Rijndael) algorithm is the optimal method to encrypt and decrypt the data. The AES (Rijndael) utilised 256-bit keys with flexible and efficient operation speed and could be applied in various platforms, especially small mobile devices (Mitali and Sharma, 2014). Shafagh (2015) also stated that compared to DES and RSA, the AES has larger key size than DES and has faster encryption and decryption speed than RSA.

5.2 **Cloud provider's identity**

During driving, the car requires connecting to various cloud providers to obtain the updated traffic map and commands. If the cloud provider is not reliable, or even hackers acted like an authentic provider, the gained map and command information may lead to some terrible accidents. Therefore, the self-driving car technique requires verifying the identity of the cloud provider. The key distribution system is the selection to apply to this circumstance, which is able to ensure the cloud provider is reliable. The key distribution center (KDC) shares a pair of unique master keys with users through the physical transmission, and when users proceed communications, they have to apply for the exclusive session key from the KDC, which is encrypted by the master key of KDC (Levi and Sarimurat, 2017).

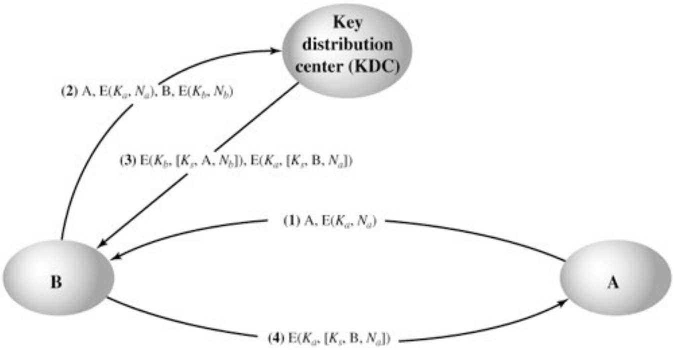
Key distribution center (KDC)
(2) A, E(K_a, N_a), B, E(K_b, N_b)
(3) E(K_b, [K_s, A, N_b]), E(K_a, [K_s, B, N_a])
(1) A, E(K_a, N_a)
B
A
(4) E(K_a, [K_s, B, N_a])

Figure (6). The key distribution scheme (Avaliable on http://flylib.com/books/en/3.190.1.71/1/).

5.3 **Information integrity**

Information integrity, as one of the most significant security requirements of IoT, is able to guarantee that all the collected data are reliable and integrated (Xu, Wendt and Potkonjak, 2014). Some sensors of IoT have the data gathering rate with low real-time delay and high bandwidth features, thus, increasing some data integrity techniques to these sensors not only ensures the velocity but also reduces the external interference (Xu, Wendt and Potkonjak, 2014). In order to figure out the integrity issues, we added two protocols to the communication which are suitable for tradition network, but also appropriate for the IoT infrastructure, TLS (Transport Layer Security) and DTLS (Datagram Transport Layer Security).

As the figure shown below, the TLS contains the server, the client and the channel.

- Server: The server is to monitor the connections from the client and generate a TLSChannel instance to operate these connections (Tiburski et al., 2017).
- Client: When caught a connection, TLSClient sends the message to the Middleware Core (Tiburski et al., 2017).
- Channel: Created by the server and generate a handshake with TLSClient (Tiburski et al., 2017).

By contrast, the DTLS consists of the server, the client and the connector.

- Server: The server is to open the connection channel with the client and transfer the data (Tiburski et al., 2017).
- Client: Start the handshake with the server, receive and send message to the server (Tiburski et al., 2017).
- Connector: Guarantee the encryption, decryption, key and message exchange between the server and client. (Tiburski et al., 2017).

In both TLS and DTLS protocols, after the handshake, all the message exchanges and communications are under the protection.

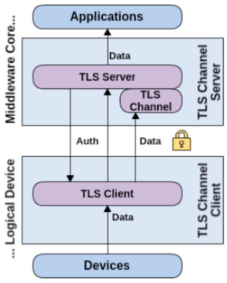

Figure (7). TLS protocol in IoT

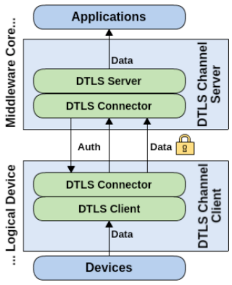

Figure (8).DTLS protocol in IoT

Note. From 'Evaluating the use of TLS and DTLS protocols in IoT middleware systems applied to E-health' (Tiburski et al., 2017).

5.4 Limitations

However, these countermeasures still have limitations. For instance, the encryption and anonymisation technique of AES (Rijndael) will encounter the brute-force attack easily due to the mathematical property (Pawar and Ghumbre, 2016). Meanwhile, Ebrahim, Khan and Khalid (2014) stated that although the AES(Rijndael) does not show any limitations, the implementation of inverse cipher through it has not illustrated adequate performance on the smart card.

For key distribution, the security level of the KDC depends on the protocol, and some simple protocols may lead to the man-in-the-middle attack (Salman et al., 2016). Secondly, the storage limitation is also the potential problem for some self-driving cars (Salman et al., 2016). Supposed there are M pairs of self-driving vehicles and clouds which are going to communicate, so we have M users and M*(M-1)/2 communications. Then, the number of session keys and master keys which need to store in the KDC increase to M*(M-1)/2 and M respectively as one communication uses one session key. Apparently, the total of keys stored in the KDC is M+M*(M-1)/2, which requires a considerable memory space. In addition, for each self-driving car, it has to store one master key and M-1 session keys. If the M is too large, the limitation of storage spaces for both KDC and self-driving car require resolving.

Moreover, the overhead of TLS and DTLS should be taken into consideration. When the TLS and DTLS first implemented, it requires buying additional equipment since it is designed for web-based applications (Tiburski et al., 2017). Through the experiment, Tiburski et al. (2017) also demonstrated the overhead increases after applying TLS and DTLS is not only relevant to the deployment of the security layer infrastructure but also the transmission and sequence of messages.

5.5 Conclusion

To sum up, the report introduced the architecture and relationship of IoT-based self-driving car and vehicular cloud, and analysed challenges and their preliminary solutions for this industry. The result of the analysis illustrated that although there exists shortage and challenges, the vehicular cloud, with the application of the cryptographic techniques, the self-driving car and related techniques are increasingly mature.

The connection between the self-driving car and vehicular cloud may encounter large amounts of security challenges. For example, confidentiality, authentication, information integrity, verification and access control. Therefore, to figure out these issues, we compared the common cryptographic algorithms and techniques in the market and selected appropriate ones for different issues. Based on the analysis results, we applied AES for solving confidentiality problems, KDC for figuring out authentication issues and TLS/DTLS for settling integrity challenges.

However, these solutions are not perfect and have limitations. It is probable that these limitations become the block of the development of the self-driving car and vehicular cloud industry. The disadvantages of them should be considered to figure out in the future.

References

Ebrahim, M., Khan, S., & Khalid, U. B. (2014). Symmetric algorithm survey: a comparative analysis. *arXiv preprint arXiv:1405.0398*.

Flylib.com. (2017). *Section 7.5. Recommended Reading and Web Sites - Cryptography and Network Security (4th Edition)*. [online] Available at: http://flylib.com/books/en/3.190.1.71/1/ [Accessed 18 Oct. 2017].

Fast Company. (2017). *The First Study Of Self-Driving Car Crash Rates Suggests They Are Safer | Fast Company*. [online] Available at: https://www.fastcompany.com/3055356/the-first-study-of-self-driving-car-crash-rates-suggests-they-are-safer [Accessed 18 Oct. 2017].

Greenberg, A.(2015). *Hackers Remotely Kill a Jeep on the Highway—With Me in It*. [online] WIRED. Available at: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ [Accessed 7 Oct. 2017].

He, W., Yan, G. and Xu, L. (2014). Developing Vehicular Data Cloud Services in the IoT Environment. *IEEE Transactions on Industrial Informatics*, 10(2), pp.1587-1595.

Jeremy, S., John, M., Brett Y, Mitchell,S., Abdullah, A., Kelvin,B., and Jordan,Hartman. CyberSecurity Considerations for an Interconnected Self-Driving Car System of Systems.

Levi, A. and Sarimurat, S. (2017). Utilizing hash graphs for key distribution for mobile and replaceable interconnected sensorsin the IoT context. *Ad Hoc Networks*, 57, pp.3-18.

Mario, G., Eun-Kyu, L., Giovanni, P, and Uichin L. (2014). Internet of Vehicles: From Intelligent Grid to Autonomous Cars and Vehicular Clouds. *World Forum on Internet of Things*

Mekki, T., Jabri, I., Rachedi, A. and ben Jemaa, M. (2017). Vehicular cloud networks: Challenges, architectures, and future directions. *Vehicular Communications*, 9, pp.268-280.

Mitali, V. K., & Sharma, A. (2014). A survey on various cryptography techniques. *International Journal of Emerging Trends and Technology in Computer Science*, *3*(4), pp. 307-312.

Pawar, A. and Ghumbre, S. (2016). A survey on IoT applications, security challenges and counter measures. 2016 International Conference on Computing, Analytics and Security Trends (CAST).

Salman, O., Abdallah, S., Elhajj, I., Chehab, A. and Kayssi, A. (2016). Identity-based authentication scheme for the Internet of Things. *2016 IEEE Symposium on Computers and Communication (ISCC).*

Shafagh, H. (2015). Toward computing over encrypted data in IoT systems. *XRDS: Crossroads, The ACM Magazine for Students*, *22*(2), pp.48-52.

Tiburski, R., Amaral, L., de Matos, E., de Azevedo, D. and Hessel, F. (2017). Evaluating the use of TLS and DTLS protocols in IoT middleware systems applied to E-health. *2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC).*

Whaiduzzaman, M, Sookhak, M, Gani, A, & Buyya, R 2014, A survey on vehicular cloud computing, Journal Of Network And Computer Applications, 40, pp. 325-344, ScienceDirect, EBSCOhost, viewed 07 October 2017.

Xu, T., Wendt, J. and Potkonjak, M. (2014). Security of IoT systems: Design challenges and opportunities. *2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD).*

Yan, G., Wen, D., Olariu, S. and Weigle, M. (2013). Security challenges in vehicular cloud computing. *IEEE Transactions on Intelligent Transportation Systems*, 14(1), pp.284-294.

Zhao, K. and Ge, L. (2013). A Survey on the Internet of Things Security. *2013 Ninth International Conference on Computational Intelligence and Security.*