International Journal of Computational and Experimental Science and ENgineering (IJCESEN)

Vol. 10-No.4 (2024) pp. 1282-1289
http://www.ijcesen.com

ISSN: 2149-9144

Research Article

Secure Drone Communications using MQTT protocol

Sushma Polasi[1]*, Hara Gopal Venkata Vajjha[2]

[1]Vignana Bharathi Institute of Technology, Associate Professor, Department of Computer Science and Engineering (Cyber Security), Aushapur, Ghatkesar.
* **Corresponding Author Email:** polasi.sushma@gmail.com - **ORCID:** 0009-0000-4943-5767

[2]Formerly Professor, Department of Statistics, Osmania University,
Email: haragopal_vajjha@yahoo.com - **ORCID:**0000-0002-3267-0688

Article Info:

DOI: 10.22399/ijcesen.685
Received : 25 November 2024
Accepted : 28 November 2024

Keywords :

Encryption algorithm,
MQTT protocol,
Drones security,
Cyber security,
UAV secure communications.

Abstract:

With the revolutionary change in emerging technologies, the usage of drones or unmanned aerial vehicles (UAV) has exponentially increased in different sectors like Industry, healthcare, military, agriculture, real estate, manufacturing, logistics, energy and many more utilities. This rapid growth creates a concern for the secure communication between the internal communication modules and the ground based computer system used for controlling the UAV. Intruder can hack into the device and attack the internal communication device with the injection of the malicious code which can lead to the malfunction of the aircraft. Security issues related to the communication between the internal modules of the drone and the ground based computer system is of major concern and is crucial. UAVs have to operate in constrained networks with limited bandwidth. In such a constrained environment MQTT protocol can be an excellent protocol. No cryptographic techniques are used to retain the simplicity and the light weight of the MQTT protocol. This contributes for the large scope for emerging with new solutions in the protection issues of MQTT communications. This paper mainly focuses on Armstrong number encryption standard algorithm for providing a computationally simple yet a secure and strong algorithm for UAVs encryption and decryption process on the communication links using MQTT protocol.

1. Introduction

Main UAVs are the autonomously operating aircrafts without an onboard human pilot. Origin and association of UAVs usage is typically was for a long duration with defence and military. These aircraft were initially used as practicing for targeting anti-aircraft missiles, data gathering and more controversially, weapons platforms[1]. Rapid growth in advanced technologies have increased the manufacturing of different types of modern UAVs that may be used for a variety of native applications, including traffic monitoring, weather update, agriculture, photography, remote sensing, search and rescue, fire fighting, and delivery of items [2,3]. Unmanned Aerial Vehicles are flying aircrafts attached to sensors and cameras. They present a range of applications such as surveillance, monitoring, delivery services, aerial photo and video capture, and more. These drones are controlled from a ground-based computer system called as ground control station and when they are out of line of sight, communication take place through the satellite. These communication lines can be prone to cyberattacks. Many protocols that are used in this communication can provide different security measures for these communications. UAVs are constrained devices which may have to work in low bandwidth networks and less battery power. An efficient protocol which supports these constrained devices is MQTT.

MQTT (Message Queuing and Telemetry Transport) protocol is designed for devices which work on low bandwidth networks and also have many constrains like low power, memory etc. [4-51]. MQTT can efficiently work in UAV for Control and telemetry, specifically for publishing GPS coordinates altitude, battery level and any other sensor data. MQTT can further simplify unmanned traffic management by publishing location and status information to the Fleet management application. In image and video streaming MQTT can be used for publishing small commands or metadata related to the image and video streams like triggering the UAV to start recording the video or give video

stream relevant information such as frame rate and resolution. In edge computing MQTT can be used to send data from the aircraft to an edge computing device, such as a Raspberry Pi where it can be further processed in real-time.

2. Unmanned aerial Vehicles Architecture

General purpose UAVs consists of majorly three modules [50]:

- The drone/aircraft
- Communication links
- Ground based control station

Aircraft have components that help it move and fly, move and stand steadily in the air. Few of the components that are important for the UAV flight are the flight controller, altimeter, rotor, body frame, transmitter, power supply panel, receiver and battery. It is also accomplished with sensors and actuators.A Ground control station (GCS) can be an application on the portable Ground control station like a mobile phone or a two or more computer systems basically used for controlling the flight of the unmanned aerial vehicles.
Data communication link is crucial for secure communications between the drone and the ground based computer systems which is called as ground control station. Aircraft can communicate to GCS by using 3G, 4G, 5G, WiFi, Bluetooth etc. [16]. The commands are given to aircraft by the GCS using this communication link. Malfunctioning of communication link lead to disconnection of UAV and the GCS. Figure 1 depicts the UAV Architecture.

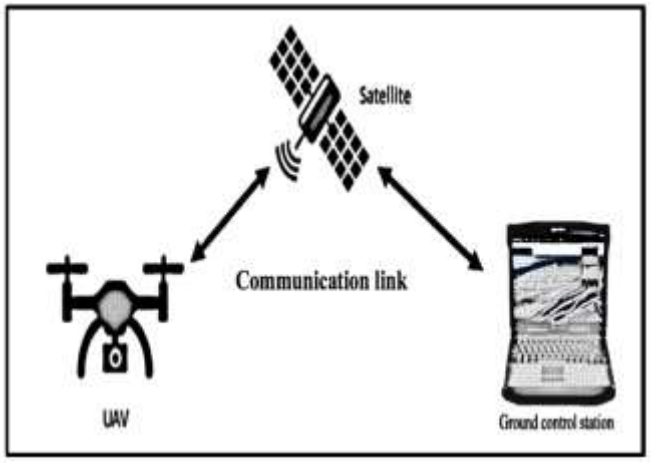

Figure 1. *UAV architecture*

3. Literature survey

Many researchers have contributed to the security of the UAVs in various ways. Yousuf et. al presented issues related to efficient transmission of data in big data and cloud computing services and security. Authors further discussed about the fully homomorphic encryption, its evolution and usage in the recent years for ensuring the confidentiality and security [12].
Authors Alladi et.al. presented a formal security analysis and cryptanalysis along with the proposal of a protocol which provides security mechanisms like authentication, user anonymity etc. Which could address the security threats like masquerade, reply attack, tampering, attacks involving cloning etc. Behaviour of the protocol proposed by authors is compared with the present day authentication protocols of the drone based on the different factors like communication, computation and storage cost [14].
Lakew et. al. Made an assessment of security threats for the two drones Parrot mambo FPV and Machine E010. Authors also discussed about the solutions and the necessary measures to enhance the resilience of the UAVs against the recognized risks by imitating a attack called as man in the middle injection attack on the control command to attack the drone[18].
Fotohi et. al. presented the results after performing the exploit on the commercially available aircrafts. Authors further proposed an intrusion detection system to secure the aircraft from the variety of cyber threats and vulnerabilities using the human immune system[19].
Zhao et. al. revealed that the high band frequency aircrafts with more than 60GHz performed better in identifying intrusion attack on 2.5GHz-5GHz drones with low frequency. Further authors discussed about the line of sight(LoS) and non-line of sight(non-LoS) cyber threats and vulnerabilities with respect to antennas and electromagnetic wave propagation in the UAVs[20].

4. Cyber threats for the UAV communications

With the fast evolving technologies, eliminating the vulnerabilities is a greater task. It is always an essential part of every application that is developed. There is high need for vulnerabilities to be identified and addressed for secure communication. Common types of UAVs attacks that can interrupt the communications in the aircraft are Man in middle attack, spoofing, Denial of service, packet attacks etc.

- Spoofing: An attack on authentication and is masquerading a communication or message from an unknown entity as being from known trusted entity. UAVs communication can be sent a counterfeit signal, resembling an original signal. If the intruder makes a valid connection, he will be able to spoof almost every function of the aircraft [33].
- Man in middle attack: Impersonating of data by eavesdropping in the middle of the communication is the man in middle attack. Intruder can capture the

communication between the GCS and UAV and make the necessary modification to the packets messages or commands thereby causing a loss to UAVs.

- Denial of service attack: this attack can block the communication of the UAV by making the aircraft unavailable for some period of time by pumping the huge number of packets into the communication line or to the device. When intruder uses multiple source for the same it is Distributed denial of service. This can cause many unforeseen consequences to the aircraft [34].
- Packet attack: Collection of digital data transfer in a particular sequential manner is a packet. A packet when transferred in a greater size than the capacity of the receiver floods the receiver [35]. When the intruder injects a packet into the communication line with the malicious code, it can cause receiver from being compromised. If the receiver further processes and forges causing the sensitive information from getting destroyed or disrupting the network [36]. Packet injection can cause aircraft communication beacon frames from being captured which contain all the sensitive information related to the wireless network channel, aircraft MAC address, remote control device [37].

5. Proposed approach

The rapid increase in applications of drones in different sectors proportionally increased the cyber threats. The need for a secure and a simple techniques for securing the communication has drastically increased. With a simple and light weight protocol like MQTT the communications can be made secure.

MQTT protocol works with SSL/TLS for providing security but this increases the packet size. Transport layer services can be forgone by simply encrypting the packets of application layer thereby increasing the efficiency in terms of power consumption, security and usage of network bandwidth. For constraints devices like aircrafts retaining a smaller packet size is quite important. This paper proposes and computationally simple, yet a strong encryption algorithm called Armstrong Number Encryption Standard algorithm(ANES). This algorithm uses binary data for encryption and decryption. ANES uses the technique of chaining for encrypting and decrypting the data on communication links. ANES uses three different values as a secret key for converting binary text to cipher text. They are Armstrong number, random number as initialization vector and the packet data size. A change in a single bit can be identified with the chaining factor in the algorithm. This factor help the receiver to easily identify the compromised data. There is not scope for reply attack as a same to text doesn't generate the same cipher text because of the randomly changing initialization vector. Figure 2 is the proposed UAV architecture.

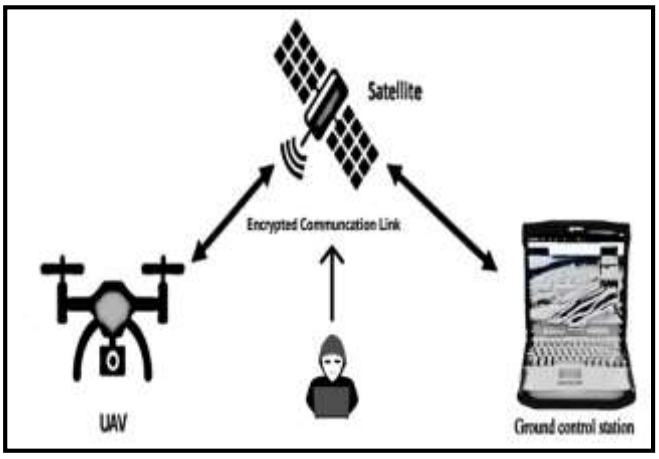

Figure 2. *Proposed UAV architecture*

Working principle of ANES include the simple operations like, XOR, Circular right and left shifts. These operations retain the simplicity of the algorithm. Every block of plain text and previous block of cipher text are XORed and encrypted. The block size in the encryption process is of arbitrary size.

The algorithm keeps the sessions unpredictable by the intruder as the block size and random number constantly vary. The packets transmitted on the communication links remains encrypted using ANES.

Encryption algorithm

Step 1:

Let n1,n2,n3……ns-1,ns be the binary stream plain text which is separated into 's' successive 'b' blocks.

0 bits are parsed to the final block to make it equivalent to the other block of size 'b' bits.

Step 2:

let 'r' be computed as quotient of the following division operation:

[Total number of bits in each binary bit block]/[Total number of binary blocks]

On the initial block perform the following:

'r' times- the circular left shift operation is performed and then the resultant and the Armstrong number 'k' are XORed to obtain 'm1'

Say 'm1' as the result of the Step 2.

6.Mathematical Approach

6.1 Encryption process

Step 3:

Let 'IV' be the initialization vector which is a number generated randomly. Figure 3 is the ANES encryption.

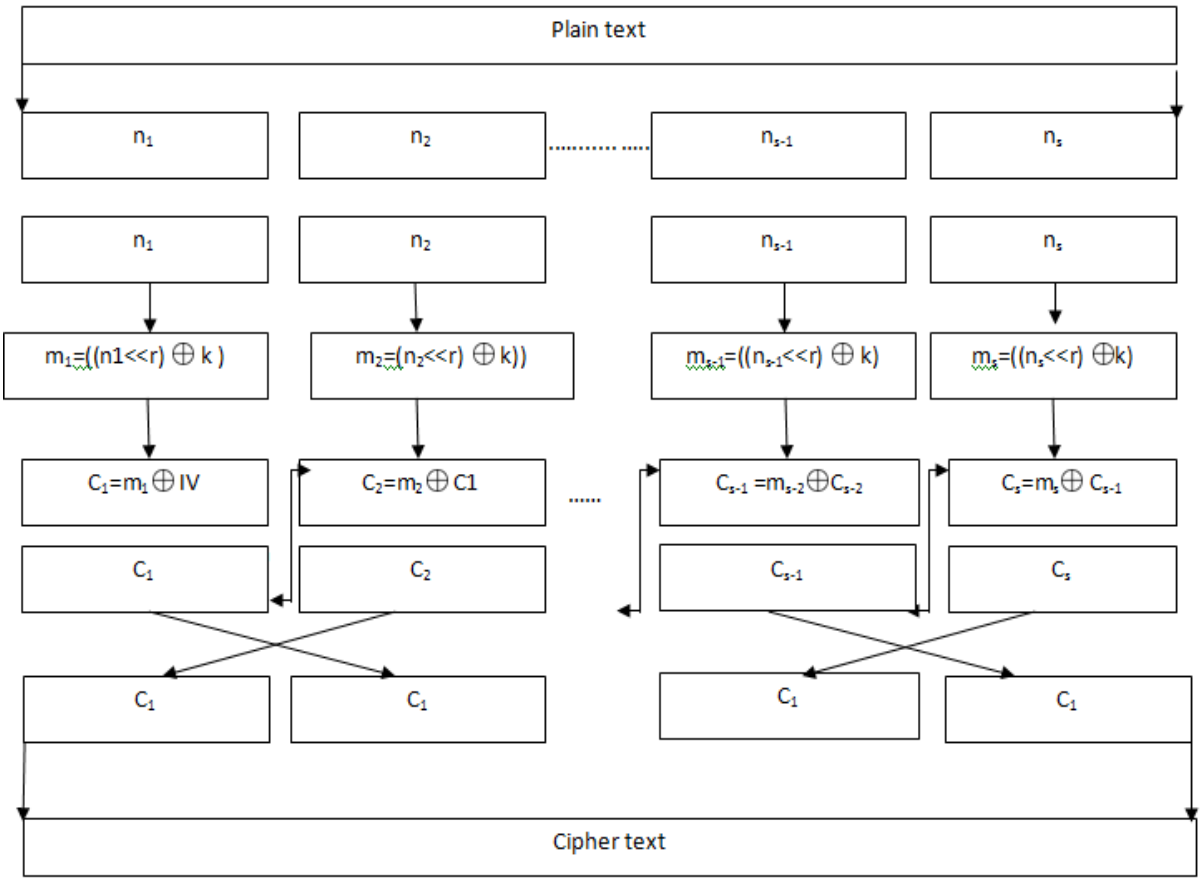

Figure 3. *ANES encryption*

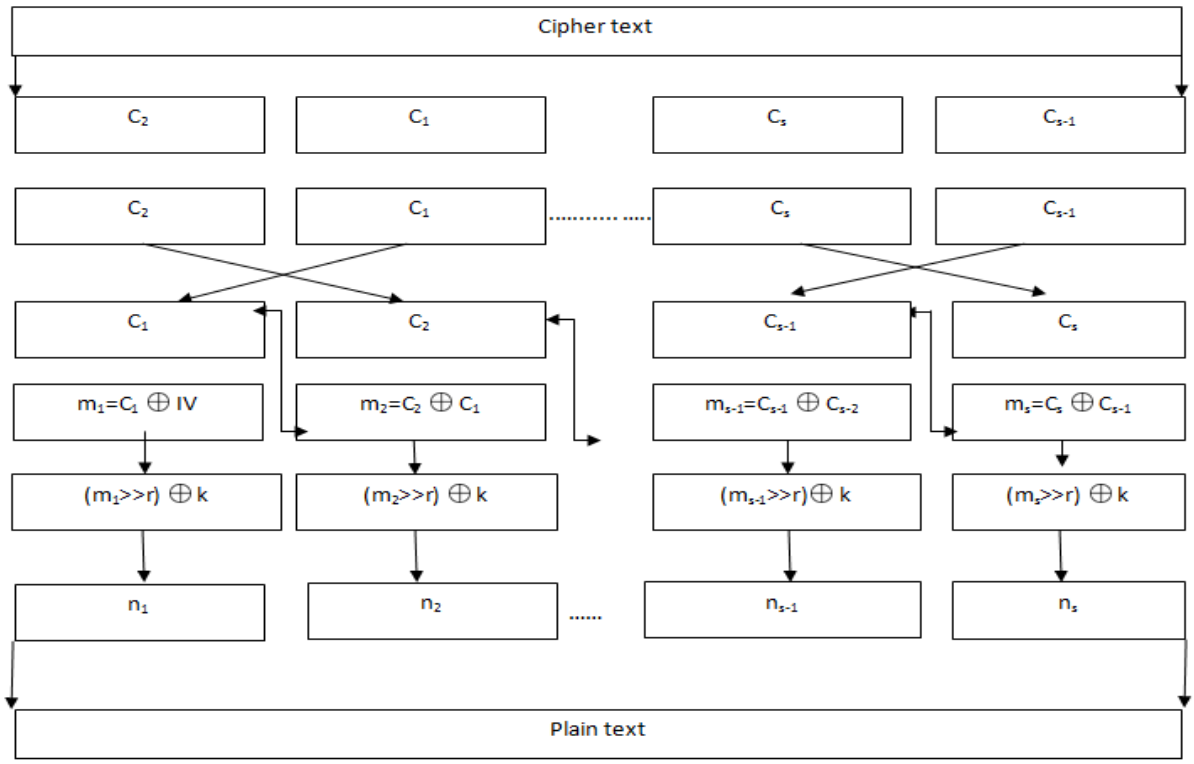

Figure 4. *ANES Decryption*

6.1 Decryption process

The result of step 2 ‘m1’ and ‘IV’ are XORed to generate the initial Cipher block, ‘C1’.

In every encryption process the initialization vector can be changed making the algorithm stronger.

Step 4:

Similarly, generate the remaining cipher blocks.

Perform transformation operation by interchanging the blocks as follows:

- Interchange the first and the second blocks
- Interchange the third and the fourth block

This process continues for all the blocks

Last block will be interchanges with last but one block.

If the number blocks are odd, then the last block is concatenated without interchanging it with other blocks.

Step 5:

C1,C2, …..Cn-1,Cn are the cipher text blocks which is considered as ‘C’ the cipher text on the whole.

‘C’ is transmitted to the destination , the ground control manager.

Decryption algorithm

Step 1:

The receiver, the ground control manager, receives the encrypted text ‘C’(Cipher text).

‘C’ is divided into multiple blocks of size ‘b’ . Let the total number of blocks be ‘s’.

Let the blocks be C1, C2, ……..Cs-1, Cs.

Step 2:

The cipher blocks are set in proper order by performing reverse transformation. Exactly opposite to the encryption process as follows.

- First block is interchanged with second block.
- Third block is interchanged with fourth block

This process continues for all the blocks.

Last block will be interchanges with last but one block.

If the number blocks are odd, then the last block is considered the way it is without any interchanging.

Step 3:

Initialization vector ‘IV’ which is a random number is XORed with the C1, first cipher block. Let the result be the block ‘m1’.

- C1 will be initialization vector for C2,
- C2 will be IV for C3,
- Similarly Cs-1 will be IV for Cs.

The result will be series of blocks m1,m2……ms-1, ms.

Step 4:

The resultant blocks of Step 2 and the Armstrong number ‘k’ are XORed.

And finally, perform circular left shift to obtain the plain text binary blocks.

Step 5:

The above procedure is repeated for all the remaining blocks.

Finally the plain text binary blocks n1, n2…….ns-1, ns will be obtained.

A chaining process is followed to obtain the remaining blocks. Previous block of cipher will serve the purpose of initialization vector for the next block. ANES is experimentally check with different sets of data with varying payload lengths. The algorithm is implemented using python[20]. And the time is noted for the data with different sizes. The time taken are displayed in the table 1. Figure 4 shows the ANES decryption.

Table 1. *statistical analysis of encryption and decryption process in ms.*

length	~5000	~8000	~10000	~30000	~50000	~70000	~90000
Time taken for encryption in ms	34	78	89.76	463.01	1375.45	2423.89	3714.19
Time taken for decryption in ms	33	60.77	65	472.55	1301.47	2596.74	3533.27
over all time taken in ms	67	138.77	154.76	935.56	2672.92	5020.63	7247.46
Average time taken in ms	0.67	1.39	2	9	27	50	72

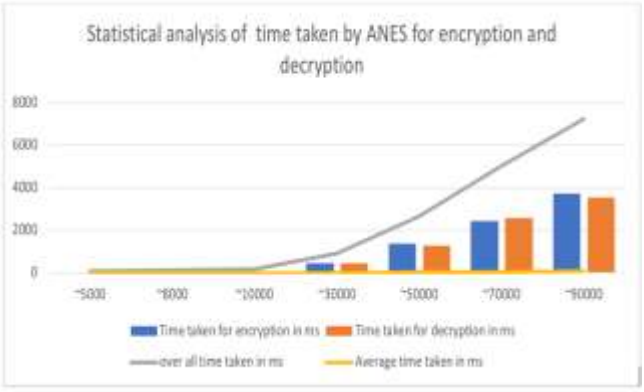

Figure 5. *Payload size vs time taken for encryption and decryption comparative study.*

Time complexity of different algorithms is also considered to evaluate the performance of the ANES algorithm.

With the above analysis, though AES is preferred for established security and compatibility with the light weight encryption mode for UAVs , ANES has a potential advantages if it is offered with specialized optimization or features tailored with MQTT and

UAV specific communication , balancing performance security and efficiency against the AES.

ANES works potentially well for the smaller messages with respect to the AES in the UAV communication. While figure 5 is the payload size vs time taken for encryption and decryption comparative study, the table 2 is time complexity of encryption algorithms. Cyber security is a popular nowadays and it has been reported a number of works on this topic [52-58].

***Table 2**. Time complexity of encryption algorithms*

Algorithm	Time complexity
AES	O(m) m is message
DES	O(m)
RSA	Same structure O(m) Different structure O(mn) n is number of plain text blocks
ANES	O(s.b+|c|) s is number of blocks b is size of each block in bits |c| size of cipher text in bits or bytes

7. Conclusion

Armstrong number encryption standard is proposed to secure UAV communications from being compromised between the ground based computer systems and the drone. Thereby securing the communications from the eavesdroppers impersonating the data by sending fake commands to UAV or even taking control over the aircraft. ANES encryption is a strong yet computationally simple technique to provide the security of the data communications between the UAV and GCS.

Experiments have been conducted on different sizes of payload to check the efficiency. Decryption processes is faster than the encryption because of the technique used in algorithm. This algorithm serves as a best purpose for retaining the confidentiality and addressing the man in middle attack. Computationally, ANES algorithm works in an efficient manner on the drones as the operations considered in this algorithm are restricted to basic XOR and Circular left and right shifts.

This algorithm works effectively and efficiently on constrained devices like drones where the storage space, battery usage for computation are considered on the priority basis.

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

[1]Gupta SG, Ghonge D, Jawandhiya PM (2013). Review of unmanned aircraft system (UAS). *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)* 2;4. http://dx.doi.org/10.2139/ssrn.3451039

[2]Hiebert B, Nouvet E, Jeyabalan V, Donelle L. (2020). The application of drones in healthcare and health-related services in north america: A scoping review. *Drones.* 4(3):30.

[3]Tomic T, Schmid K, Lutz P, Domel A, Kassecker M, Mair E, Grixa IL, Ruess F, Suppa M, Burschka D. (2012). Toward a fully autonomous UAV: Research platform for indoor and outdoor urban search and rescue. *IEEE robotics & automation magazine*. 19(3);46-56. DOI: 10.1109/MRA.2012.2206473

[4]Hartmann K, Steup C. (2013). The vulnerability of UAVs to cyber attacks-An approach to the risk assessment. *5th international conference on cyber conflict (CYCON 2013)* (pp. 1-23).

[5]Snead J, Seibler JM, Inserra D. (2018). Establishing a legal framework for counter-drone technologies. *Heritage Foundation;* 3305 http://report.heritage.org/bg3305

[6]Zeng Y, Wu Q, Zhang R. (2019). Accessing from the sky: A tutorial on UAV communications for 5G and beyond. *Proceedings of the IEEE.* 107(12):2327-75.

[7]Vergouw B, Nagel H, Bondt G, Custers B. (2016). Drone technology: Types, payloads, applications, frequency spectrum issues and future developments. *InThe future of drone use* (pp. 21-45). TMC Asser Press, The Hague.

[8]Yağdereli E, Gemci C, Aktaş AZ. (2015). A study on cyber-security of autonomous and unmanned vehicles. *The Journal of DefenseModeling and Simulation*. 12(4):369-81. https://doi.org/10.1177/1548512915575803

[9]Khan N, Abdullah J, Khan AS. (2017). Defending malicious script attacks using machine learning classifiers. *Wireless Communications and Mobile*

Computing. 2017;5360472, 9 pages https://doi.org/10.1155/2017/5360472

[10]Alqarni AA, Alsharif N, Khan NA, Georgieva L, Pardade E, Alzahrani MY (2022). MNN-XSS: Modular neural network based approach for XSS attack detection. *Computers, Materials and Continua*. 70(2):4075-85.

[11]Rugo A, Ardagna CA, Ioini NE. (2022). A Security Review in the UAVNet Era: Threats, Countermeasures, and Gap Analysis. *ACM Computing Surveys (CSUR).* 55(1);1-35. https://doi.org/10.1145/3485272

[12]Yousuf H, Lahzi M, Salloum SA, Shaalan K. (2021). Systematic review on fully homomorphic encryption scheme and its application. *Recent Advances in Intelligent Systems and Smart Applications*. 537-551. DOI:10.1007/978-3-030-47411-9_29

[13]Brakerski Z, Döttling N, Garg S, Malavolta G. (2020) Candidate iO from homomorphic encryption schemes. *InAnnual International Conference on the Theory and Applications of Cryptographic Techniques* Springer, Cham. (pp. 79-109).

[14]Alladi T, Bansal G, Chamola V, Guizani M. (2020) Secauthuav: A novel authentication scheme for uav-ground station and uav-uav communication. *IEEE Transactions on Vehicular Technology.* 69(12):15068-77

[15]Chaari L, Chahbani S, Rezgui J. (2020). MAV-DTLS toward security enhancement of the uav-gcs communication. In2020 *IEEE 92nd Vehicular Technology Conference (VTC2020-Fall).*

[16]Islam N, Rashid MM, Pasandideh F, Ray B, Moore S, Kadel R. (2021). A review of applications and communication technologies for internet of things (IoT) and unmanned aerial vehicle (uav) based sustainable smart farming. *Sustainability.* 13(4);1821 https://doi.org/10.3390/su13041821

[17]Chamola V, Kotesh P, Agarwal A, Gupta N, Guizani M. (2021) A comprehensive review of unmanned aerial vehicle attacks and neutralization techniques. *Ad hoc networks.* 111;102324 doi: 10.1016/j.adhoc.2020.102324.

[18]LakewYihunie F, Singh AK, Bhatia S. (2020) Assessing and exploiting security vulnerabilities of unmanned aerial vehicles. *InSmart systems and IoT: innovations in computing Springer, Singapore. 141;*701-710. https://doi.org/10.1007/978-981-13-8406-6_66

[19]Fotohi R. (2020) Securing of Unmanned Aerial Systems (UAS) against security threats using human immune system. *Reliability Engineering & System Safety*. 193:106675.

[20]Sushma, P. (2024). Smart Devices Security with Armstrong Number Encryption Standard Algorithm using MQTT Protocol-An IoT Application. *International Journal of Intelligent Systems and Applications in Engineering*, 12(10s), 45–51. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/4348

[21]Thomas A, Sharma VK, Singhal G. (2015). Secure link establishment method to prevent jelly fish attack in MANET. *In2015 International Conference on Computational Intelligence and Communication Networks (CICN).* (pp. 1153-1158)

[22]Y. Li and L. Cai, (2017). UAV-Assisted Dynamic Coverage in a Heterogeneous Cellular System, in *IEEE Network*, 31(4);56-61, doi: 10.1109/MNET.2017.1600280.

[23]Steinmann JA, Babiceanu RF, Seker R. (2016) UAS security: Encryption key negotiation for partitioned data. *In2016 Integrated Communications Navigation and Surveillance (ICNS)* (pp. 1E4-1).

[24]Samland F, Fruth J, Hildebrandt M, Hoppe T, Dittmann J. AR. (2012). Drone: security threat analysis and exemplary attack to track persons. *InIntelligent Robots and Computer Vision XXIX: Algorithms and Techniques International Society for Optics and Photonics*. 8301; 83010G)

[25]Płotka M, Malanowski M, Samczyński P, Kulpa K, Abratkiewicz K. Al-Turjman F, Abujubbeh M, Malekloo A, Mostarda L. (2020) UAVs assessment in software-defined IoT networks: An overview. *Computer Communications.* 150;519-536.

[26] P. Kalpana, K. Malleboina, M. Nikhitha, P. Saikiran and S. N. Kumar, (2024). Predicting Cyberbullying on Social Media in the Big Data Era Using Machine Learning Algorithm. *2024 International Conference on Data Science and Network Security (ICDSNS)*, Tiptur, India, pp. 1-7, https://doi.org/10.1109/ICDSNS62112.2024.10691297.

[27]Lin C, He D, Kumar N, Choo KK, Vinel A, Huang X. (2018). Security and privacy for the internet of drones: Challenges and solutions. *IEEE Communications Magazine.* 56(1);64-69 DOI: 10.1109/MCOM.2017.1700390

[28]Viji D, Saravanan K, Hemavathi D. (2017) A journey on privacy protection strategies in big data. *In2017 international conference on intelligent computing and control systems (ICICCS) IEEE.* pp. 1344-1347.

[29]Gahi Y, Guennoun M, El-Khatib K. (2015). A secure database system using homomorphic encryption schemes. *arXiv preprint arXiv*:1512.03498.

[30] Kalpana, P., Anandan, R. (2023). A capsule attention network for plant disease classification. *Traitement du Signal,* 40(5);2051-2062. https://doi.org/10.18280/ts.400523

[31]Kerns AJ, Shepard DP, Bhatti JA, Humphreys TE. (2014). Unmanned aircraft capture and control via GPS spoofing. *Journal of Field Robotics.* 31(4);617-636

[32]Chen J, Feng Z, Wen JY, Liu B, Sha L. (2019). A container-based DoS attack-resilient control framework for real-time UAV systems. In 2019 *Design, Automation & Test in Europe Conference & Exhibition. IEEE*. pp. 1222-1227.

[33] P. Kalpana, P. Srilatha, G. S. Krishna, A. Alkhayyat and D. Mazumder, (2024). Denial of Service (DoS) Attack Detection Using Feed Forward Neural Network in Cloud Environment. *2024 International Conference on Data Science and Network Security (ICDSNS)*, Tiptur, India, 2024, pp. 1-4, https://doi.org/10.1109/ICDSNS62112.2024.10691181

[34]Khan N, Abdullah J, Khan AS. (2017) A dynamic method of detecting malicious scripts using classifiers.

Journal of Computational and Theoretical Nanoscience 23(6);5352-5355 DOI:10.1166/asl.2017.7374

[35]M. Pan, C. Chen, X. Yin and Z. Huang, (2022). UAV-Aided Emergency Environmental Monitoring in Infrastructure-Less Areas: LoRa Mesh Networking Approach, in *IEEE Internet of Things Journal*, 9(4);2918-2932,doi: 10.1109/JIOT.2021.3095494

[36]Schmittner C, Ma Z, Schoitsch E, Gruber T. (2015). A case study of fmvea and chassis as safety and security co-analysis method for automotive cyber-physical systems. *In Proceedings of the 1st ACM Workshop on Cyber-Physical System Security*. (pp. 69-80)

[37]Liu CH, Chen Z, Tang J, Xu J, Piao C. (2018). Energy-efficient UAV control for effective and fair communication coverage: A deep reinforcement learning approach. *IEEE Journal on Selected Areas in Communications.* 36(9):2059-2070 DOI: 10.1109/JSAC.2018.2864373

[38]Benzekki K, El Fergougui A, Elbelrhiti EA. (2016). A secure cloud computing architecture using homomorphic encryption. *International Journal of Advanced Computer Science and Applications.* 7(2):293-298. DOI:10.14569/IJACSA.2016.070241

[39]Mittal D, Kaur D, Aggarwal A. (2014). Secure data mining in cloud using homomorphic encryption. *In2014 IEEE international conference on cloud computing in emerging markets (CCEM).* (pp. 1-7)

[40]Bocu R, Costache C. (2018). A homomorphic encryption-based system for securely managing personal health metrics data. *IBM Journal of Research and Development*. 25;62(1):1-10. doi: 10.1147/JRD.2017.2755524.

[41]Acar A, Aksu H, Uluagac AS, Conti M. (2018) A survey on homomorphic encryption schemes: Theory and implementation. *ACM Computing Surveys (Csur).* 51(4);1 – 35 https://doi.org/10.1145/321430

[42]Cominetti EL, Simplicio MA. (2020). Fast additive partially homomorphic encryption from the approximate common divisor problem. *IEEE Transactions on Information Forensics and Security.* 15;2988-2998.

[43]P. Kalpana, M. Almusawi, Y. Chanti, V. Sunil Kumar and M. Varaprasad Rao, (2024). A Deep Reinforcement Learning-Based Task Offloading Framework for Edge-Cloud Computing, *2024 International Conference on Integrated Circuits and Communication Systems (ICICACS)*, Raichur, India, pp. 1-5, https://doi.org/10.1109/ICICACS60521.2024.10498232.

[44]Sharma T. (2016). E-voting using homomorphic encryption scheme. *International Journal of Computer Applications.* 141(13):14-6.

[45]Paillier P. (1999). Public-key cryptosystems based on composite degree residuosity classes. *International conference on the theory and applications of cryptographic techniques* Springer, Berlin, Heidelberg. (pp. 223-238)

[46]AVENS, Aerial Vehicle Network Simulator, Available online: https://omnetpp.org/download-items/AVENS.html

[47]Talaei Khoei, Tala & Ghribi, Elias & Prakash, Ranganathan & Kaabouch, Naima. (2021). *A Performance Comparison of Encryption/Decryption Algorithms for UAV Swarm Communications.* DOI:10.13140/RG.2.2.17379.48160

[48]Goldin, C. D., & Katz, L. F. (2008). The race between education and technology. *Belknap Press of Harvard University Press.*

[49]Auster, P. (2007). *The Brooklyn follies.* http://www.barnesandnoble.com/

[50]Akkurt I. (2022, October 28–31). Title of presented work [Conference presentation abstract]. *9th International Conference on Computational and Experimental Science and Engineering (ICCESEN 2022), Antalya-Turkey*. http://www.iccesen.org

[51]Austerlitz, S. (2015). How long can a spinoff like 'Better Call Saul' last? *FiveThirtyEight.* http://fivethirtyeight.com/features/how-long-can-a-spinoff-like-better-call-saul-last/

[52]guven, mesut. (2024). Dynamic Malware Analysis Using a Sandbox Environment, Network Traffic Logs, and Artificial Intelligence. *International Journal of Computational and Experimental Science and Engineering*, 10(3);480-490. https://doi.org/10.22399/ijcesen.460

[53]Venkatraman Umbalacheri Ramasamy. (2024). Overview of Anomaly Detection Techniques across Different Domains: A Systematic Review. *International Journal of Computational and Experimental Science and Engineering*, 10(4);898-910. https://doi.org/10.22399/ijcesen.522

[54]R, U. M., P, R. S., Gokul Chandrasekaran, & K, M. (2024). Assessment of Cybersecurity Risks in Digital Twin Deployments in Smart Cities. *International Journal of Computational and Experimental Science and Engineering*, 10(4);695-700. https://doi.org/10.22399/ijcesen.494

[55]Prasada, P., & Prasad, D. S. (2024). Blockchain-Enhanced Machine Learning for Robust Detection of APT Injection Attacks in the Cyber-Physical Systems. *International Journal of Computational and Experimental Science and Engineering*, 10(4);799-810. https://doi.org/10.22399/ijcesen.539

[56]Alkhatib, A., Albdor , L., Fayyad, S., & Ali, H. (2024). Blockchain-Enhanced Multi-Factor Authentication for Securing IoT Children's Toys: Securing IoT Children's Toys. *International Journal of Computational and Experimental Science and Engineering*, 10(4);1041-1049. https://doi.org/10.22399/ijcesen.417

[57]C, A., K, S., N, N. S., & S, P. (2024). Secured Cyber-Internet Security in Intrusion Detection with Machine Learning Techniques. *International Journal of Computational and Experimental Science and Engineering*, 10(4);663-670. https://doi.org/10.22399/ijcesen.491

[58]Guven, M. (2024). A Comprehensive Review of Large Language Models in Cyber Security. *International Journal of Computational and Experimental Science and Engineering*, 10(3);507-516. https://doi.org/10.22399/ijcesen.469