Hybrid Cryptographic Technique of Data Security for UAV Applications

Priti Mandal
Dept. Of ECE
NIT Rourkela
Rourkela, India
pritimandal2310@gmail.com

Lakshi Prosad Roy
Dept. Of ECE
NIT Rourkela
Rourkela, India
royl@nitrkl.ac.in

Santos Kumar Das
Dept. Of ECE
NIT Rourkela
Rourkela, India
dassk@nitrkl.ac.in

Abstract— Unmanned Aerial Vehicles (UAVs) are utilised in many various sectors nowadays, including military, search and rescue, and monitoring. Although there are many applications for UAVs, security has always been a top priority. Additionally, UAVs carry private information that is sensitive and poses serious risks if criminal attackers use them to their advantage. There have been numerous attempts to address UAV security issues, but there is no established method for shielding UAVs from online threats. The increased use of UAVs has prompted us to look into their security measures, particularly user authentication. In this work, new cryptographic algorithm is proposed for securely transmitting and receiving the data. Further, the proposed algorithm is analysed based on the encryption time, decryption time, throughput, and security analysis based on avalanche effect.

Keywords—Decryption, Encryption, Security, Unmanned Aerial Vehicle (UAV).

I. Introduction

Drones, also known as unmanned aerial vehicles (UAVs), are aircraft that are remotely piloted from a location on the ground. Recently, this technology has been gaining more and more attention in military applications ranging from defence to armed attacks, and more and more states throughout the world are using it. UAVs were initially created at the turn of the 20th century as test dummies for aircraft, and they later saw inadvertent use in target practise and as decoys [1]. Later on, when UAVs were used for Intelligence, Surveillance, and Reconnaissance, their use increased. They have been weaponized since the beginning of the twenty-first century in order to attack targets. In this effort, we primarily concentrate on unarmed military UAVs for operational military applications like as military patrol and defence.

The Ground Control Station (GCS) serves as a monitoring and command station for the UAV operation, allowing operators on the ground to issue mission instructions and keep an eye on the progress of the mission and the UAV's health while it is in the air. According to research findings, Man-in the-Middle attacks can still be carried out using professional UAVs [2]. It is necessary to provide the data securely in order to prevent the attacker from reading the data sent.

The risks of cyber and electronic attacks against military UAVs are discussed in [3], particularly high-profile occurrences like the collection of unencrypted multimedia data from UAVs, which constitutes an indirect threat to security and safety. Lack of security safeguards makes UAVs much more vulnerable to cyber and electronic attacks, increasing the chance that confidential data will be misused or intercepted. Defence against complex cyber or electronic threats, such as data connection interception and navigational spoofing, is what is meant by protecting military UAVs. To stop enemy drone operations, this calls for aggressive action. This is referred to as cyber power in military operations.

The primary use of this research is counter-UAV for anti-UAV monitoring measures against external UAV assaults and unlawful use of UAVs, even in dangerous circumstances [4]. In order to defend army tanks and patrols from aerial attacks conducted by UAVs in high profile areas, a proactive counter-UAV system is required to develop. In this context, it is unquestionably crucial to monitor and analyse the data acquired by the sensors such as radar, microphone, and camera, etc.

Recent literature studies on multimedia data streaming systems have focused on scenarios with lots of nodes. With applications in aerial monitoring, search & rescue, and disaster relief, the authors of [5] provide a high-level architecture for a collaborative UAV system made up of unmanned aircraft with integrated sensors, implanted processors, and networking algorithms. The authors of [6] present an aerial ad hoc network for streaming video and carry out tests on transportable source and receiver nodes for data collection from remote sensors. The information collected by the sensors needs to be protected in some way, and the authority in charge of the data may decide to use cryptographic protection. Network security and cryptography are concepts used to safeguard wireless networks and data transfer. The key component of secure data transmission over an unstable network is data security. Today data communications face the difficult challenge of data security, which affects many areas including secure communication channels, powerful data encryption techniques, and trusted third parties to manage the database. Information privacy can only be maintained using traditional encryption techniques like DNA cryptography, DES, AES, Blowfish, RSA, and others are still in use for real-time systems [7]. However, these conventional methods use a tremendous amount of computational power. Therefore, it is necessary to establish the understanding that new cryptographic methods provide a link between old and modern technologies. In order to assess data security while exchanging crucial information, in this work, new encryption, and decryption algorithms are proposed to do so.

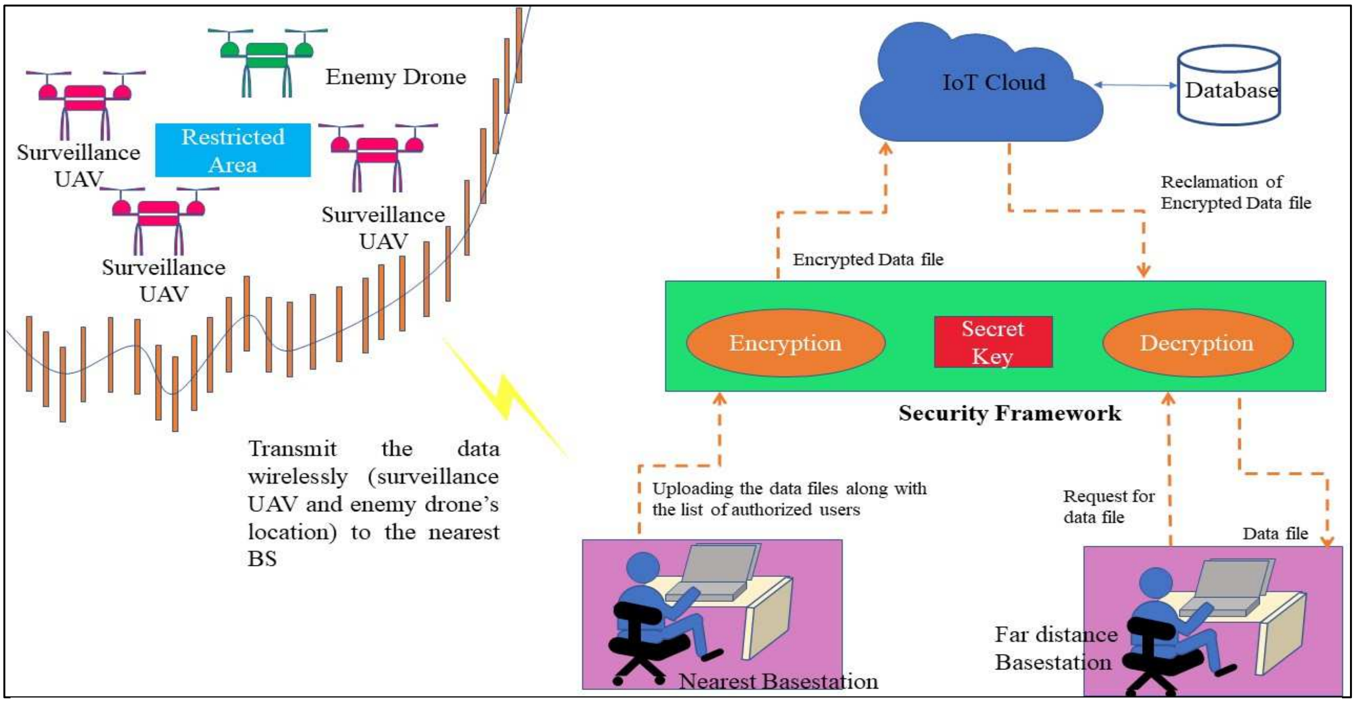

Fig.1. System Model

The remaining of the paper is organised as follows. The system model is described in Section II. The proposed encryption and decryption algorithms are covered in Section III and Section IV, respectively. Section V discusses the results and section VI finally concludes the work.

II. System Model

Considering the scenario of surveillance in any restricted area, where surveillance UAVs are patrolling to find the enemy drone if present. While monitoring surveillance drone receives the location of the enemy drone as well as other surveillance drone. The data transmission to the base-station needs to be encrypted since it contains the location information of the surveillance drone. The researchers use various techniques to transmit the information to the base-station (BS). Different BS are situated at a far distance. The nearest BS updates the data in the Internet of Things (IoT) cloud and is accessed by the far distance BS. The data transmitted to the IoT cloud are sent securely by encrypting the data to safeguard the information from jamming, spoofing, hacking, etc. In this model, the nearest BS owner uploads the file along with the list of the BS who have been granted access to the uploaded file. While uploading the data to the IoT Cloud, the security framework enquires the secret key and uses it to encrypt the data. After the encryption process, data is uploaded in the IoT Cloud. Information is stored in the database for future use. Key management is done at the security framework. To access the data by the far BS, authenticated credentials and secret key data files can be accessed. Using the secret key, the data file gets decrypted and could be used by far situated BS users. Proposed algorithms for encryptions and decryptions are explained in the following sections.

III. PROPOSED ENCRYPTION ALGORITHM

The proposed encryption algorithm is a combination of Blowfish [7] and Genetic algorithm [8]. In general, the encryption algorithm is either symmetric or asymmetric. But in this proposed encryption algorithm both the properties are taken into considerations. In this first, the data transmitted to the IoT cloud is considered as the input data $\boldsymbol{Y}$. Followed by input key is initialized. From the initialized key, $\boldsymbol{P}$ array and four substitute boxes $\boldsymbol{S}_1$, $\boldsymbol{S}_2$, $\boldsymbol{S}_3$ and $\boldsymbol{S}_4$. Then, subkeys are generated, followed by encryption and post-processing. After post-processing to make the data more secure crossover is performed using the second key. The crossover makes the encryption into asymmetric process. Secret key is formed by the left-over bits of crossover data $\boldsymbol{Y}_P$ and second key. Finally, mutation is performed for every 8th bit to form $\boldsymbol{Y}_M$ as the end product of encrypted data. Thus, it is more secure than the symmetric method and faster than the asymmetric method. The proposed algorithm for the encryption is shown in Algorithm 1. Next subsection contains the description of the proposed decryption algorithm.

IV. Proposed Decryption Algorithm

Proposed decryption algorithm is applied while retrieving the data from the IoT cloud to the BS. The reverse process of proposed encryption algorithm is applied to obtained the actual data sent by the nearer BS to the cloud. Through web application users can access the data only if secret key is available with them. Here secret key plays a crucial role. The flowchart and the proposed decryption algorithm are depicted in Algorithm 2.

V. Result And Discussion

In this section, the proposed algorithm is compared with the existing encryption techniques such as AES, DES, Blowfish and Two-fish while transmitting the data on the basis of encryption time, plain text size (i.e., data size), throughput and most importantly security analysis.

- **Encryption and Decryption Time**

Fig. 2. depicts the encryption time of the data along

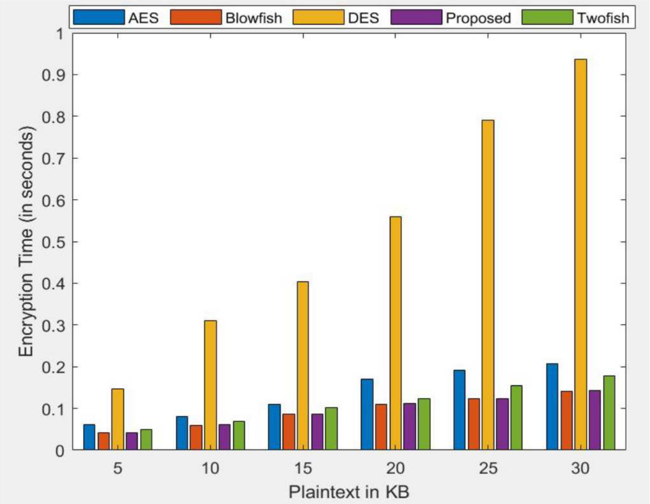

Fig. 2. Encryption time for various length of plaintext

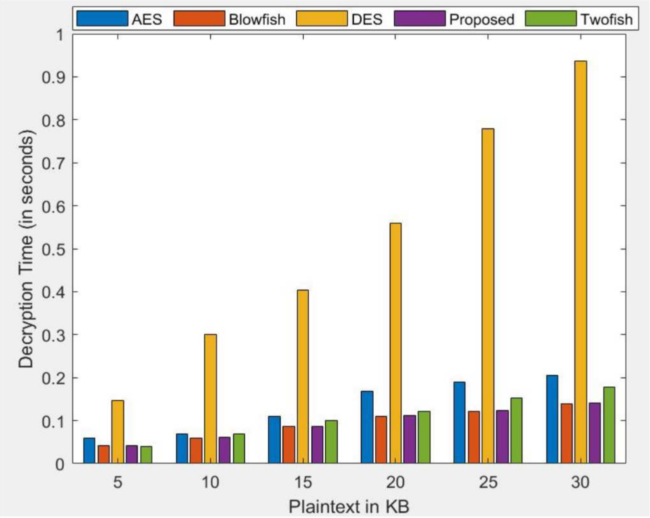

Fig. 3: Decryption time for various length of plaintext

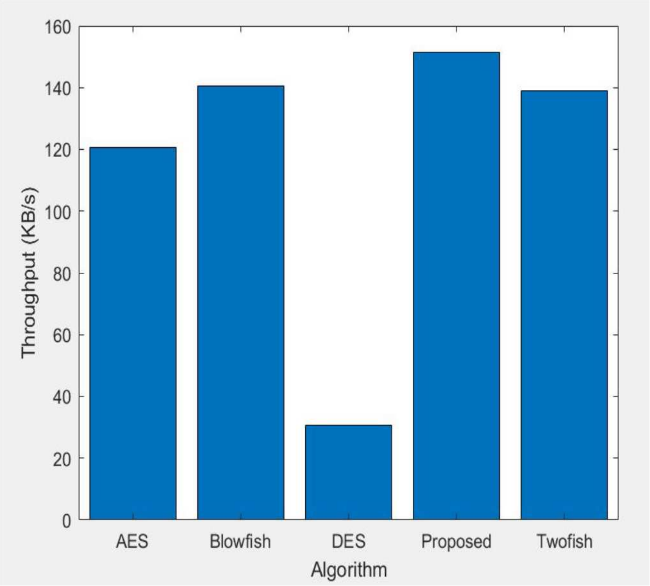

Fig. 4: Comparison of Throughput for various algorithm

Algorithm 1 Proposed Encryption Algorithm

```
Input the text of 64-bit, $\boldsymbol{Y}$.
Initialise Key input, $\boldsymbol{K_i}$
From Key input initialize $\boldsymbol{P}$ arrays, $\boldsymbol{P_i}$ and 4 Substitution
  boxes $\boldsymbol{S_1}$, $\boldsymbol{S_2}$, $\boldsymbol{S_3}$ and $\boldsymbol{S_4}$. Subkey Generation
$\boldsymbol{P}$ arrays are XORed with key bits:
    $P1 = P1\otimes$First 32 bits from Key Input
    $P2 = P2\otimes$Second 32 bits from Key Input
    $P18 = P18\otimes$Eighteenth 32 bits from Key Input
$Y$ is divided in two halves, $\boldsymbol{Y_L}$ and $\boldsymbol{Y_R}$. Encryption
for $i$ = 1 to 16
    $\boldsymbol{Y_L} = \boldsymbol{Y_L}\otimes\boldsymbol{P_i}$
    $\boldsymbol{Y_R} = f(\boldsymbol{Y_L})\otimes\boldsymbol{Y_R}$
    $\boldsymbol{Y_L}$ is divided into four 8-bits quarters: A, B, C, D
    Calculate $f$ function
    $f(\boldsymbol{Y_L})=((\boldsymbol{S_1}[\mathbf{A}]+\boldsymbol{S_2}[\mathbf{B}]\bmod 2^{32})\otimes\boldsymbol{S_3}[\mathrm{C}])+\boldsymbol{S_4}$
      $[\mathbf{D}]\bmod 2^{32}$
    Swap $\boldsymbol{Y_L}$ and $\boldsymbol{Y_R}$
end for
      Post-Processing
Again, Swap $\boldsymbol{Y_L}$ and $\boldsymbol{Y_R}$
$\boldsymbol{Y_R} = \boldsymbol{Y_R}\otimes P17$
$\boldsymbol{Y_L} = \boldsymbol{Y_L}\otimes P18$
Recombine $\boldsymbol{Y_L}$ and $\boldsymbol{Y_R}$ to form $\boldsymbol{Y_P}$
Generate second key of 64-bits
     Crossover and Mutation
Crossover is performed for $\boldsymbol{Y_P}$ and second key for
  every 8-bits to form $\boldsymbol{Y_C}$.
Secret key is formed by the left-over bits of $\boldsymbol{Y_P}$ and
  second key, $\boldsymbol{S_{Key}}$.
Mutation is done for every 8th bit of $\boldsymbol{Y_C}$ to form $\boldsymbol{Y_M}$.
```

with its size. The efficiency of the algorithm is inversely related to the time taken for the encryption. Encryption time and decryption time are evaluated at different data size 5, 10, 15, 20, 25, 30 KB for the proposed algorithm along with the existing algorithm. From the Fig. 2-3. It could be observed that proposed algorithm is much more efficient than the other existing algorithms.

- **Throughput**

Another important parameter for analysing the algorithm efficiency is throughput. Higher the throughput, greater the efficiency of the algorithm. The proposed encryption algorithm's throughput is more compared to the other algorithms. It is depicted in Fig. 4.

- **Security Analysis**

Security Analysis of the proposed algorithm is performed using avalanche effect and correlation coefficient. Avalanche effect is the property which is favourable for any encryption technique [9]. It is the evaluation of the significant change in at least half of the encrypted information due to the change in the original data or key. Fig. 5-8. depicts the avalanche effect of the proposed algorithm for the first round (FR), second round (SR) and last round (LR). Different bits number refers to the number of bits differ in cipher text when there is a change in the plain text.

Algorithm 2 Proposed Decryption Algorithm

```
De-Mutation is performed for $\boldsymbol{Y}_M$ every 8th bit forming $\boldsymbol{Y}'_M$
Perform crossover for $\boldsymbol{Y}'_M$ with $\boldsymbol{S}_{Key}$ to form $\boldsymbol{Y}'_C$.
Initialise Key input, $\boldsymbol{K}_i$
From Key input initialize $\boldsymbol{P}$ arrays, $\boldsymbol{P}_i$ and 4 Substitution boxes $\boldsymbol{S}_1$, $\boldsymbol{S}_2$, $\boldsymbol{S}_3$ and $\boldsymbol{S}_4$.
$\boldsymbol{P}$ arrays are XORed with key bits:
  $P18$ = $P18$⊗Eighteenth 32 bits from Key Input
  $P17$ = $P17$⊗Seventeenth 32 bits from Key Input
  $P1$ = $P1$⊗First 32 bits from Key Input
$\boldsymbol{Y'}_C$ is divided in two halves, $\boldsymbol{Y'}_L$ and $\boldsymbol{Y'}_R$.
  Post-processing
$\boldsymbol{Y'}_L$ =$\boldsymbol{Y'}_L$⊗P18
$\boldsymbol{Y'}_R$= $\boldsymbol{Y'}_R$⊗P17
Swap $\boldsymbol{Y'}_L$ and $\boldsymbol{Y'}_R$
  Decryption
Swap $\boldsymbol{Y'}_L$ and $\boldsymbol{Y'}_R$
for $i$ = 16 to 1
    $\boldsymbol{Y'}_L$ = $\boldsymbol{Y'}_L$⊗$P_i$
    $\boldsymbol{Y'}_R$ = $f(\boldsymbol{Y'}_L)$⊗$\boldsymbol{Y'}_R$
    $\boldsymbol{Y'}_L$ is divided into four 8-bit quarters: $\boldsymbol{A'}$, $\boldsymbol{B'}$, $\boldsymbol{C'}$, $\boldsymbol{D'}$
    Calculate $f$ function:
      $f(\boldsymbol{Y'}_L) = ((\boldsymbol{S}_1 [\mathbf{A'}] + \boldsymbol{S}_2 [\mathbf{B'}]\text{mod}2^{32}) \otimes \boldsymbol{S}_3 [\mathbf{C'}]) + \boldsymbol{S}_4 [\mathbf{D'}]\text{mod}2^{32}$
    Swap $\boldsymbol{Y'}_L$and $\boldsymbol{Y'}_R$
end for
Recombine $\boldsymbol{Y'}_L$and $\boldsymbol{Y'}_R$ to form $\boldsymbol{Y}'$
```

While the column's ratio bits indicate the ratio of the different bits number to that of the total number of bit sequence. Correlation Coefficient is the dependency of the one variable on the other. Here, the dependency of the original and the encrypted is analysed. It can be represented mathematically as [8],

$$C_{\boldsymbol{Y},\boldsymbol{Y}_m} = \frac{cov(\boldsymbol{Y},\boldsymbol{Y}_m)}{\sqrt{D(\boldsymbol{Y}).D(\boldsymbol{Y}_m)}} \tag{1}$$

$$cov(\boldsymbol{Y},\boldsymbol{Y}_m) = \frac{1}{\beta}\sum_{\alpha=1}^{\beta}(\boldsymbol{Y}_\alpha - E(\boldsymbol{Y})).(\boldsymbol{Y}_{m\alpha} - E(\boldsymbol{Y}_m)) \tag{2}$$

$$E(\boldsymbol{Y}) = \frac{1}{\beta}\sum_{\alpha=1}^{T}\boldsymbol{Y}_\alpha \tag{3}$$

$$D(\boldsymbol{Y}) = \frac{1}{\beta}\sum_{\alpha=1}^{\beta}(\boldsymbol{Y}_\alpha - E(\boldsymbol{Y}))^2 \tag{4}$$

Fig. 8. depicts that there are total 51 values out of 64, whose correlation coefficient near zero, i.e., it shows the non-linearity, 2 values are -0.3924 and -0.3863, and rest values are weak positive and negative linear relations.

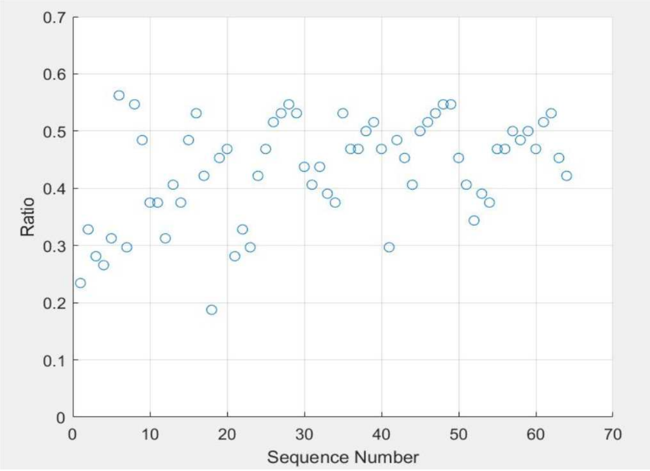

Fig. 5: Avalanche effect analysis for first round

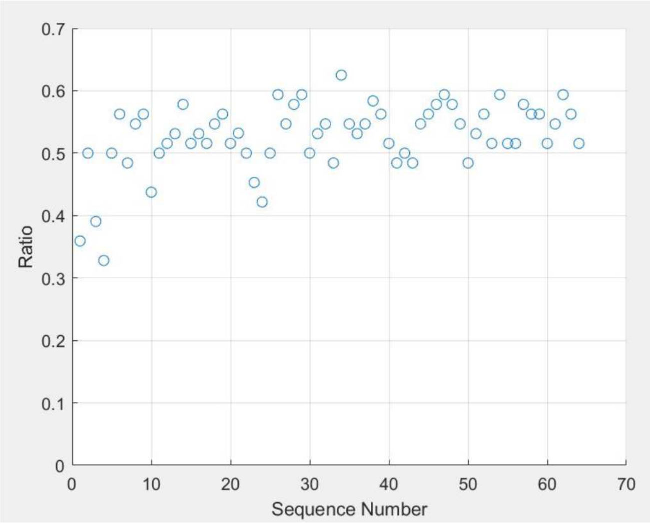

Fig. 6: Avalanche effect analysis for second round

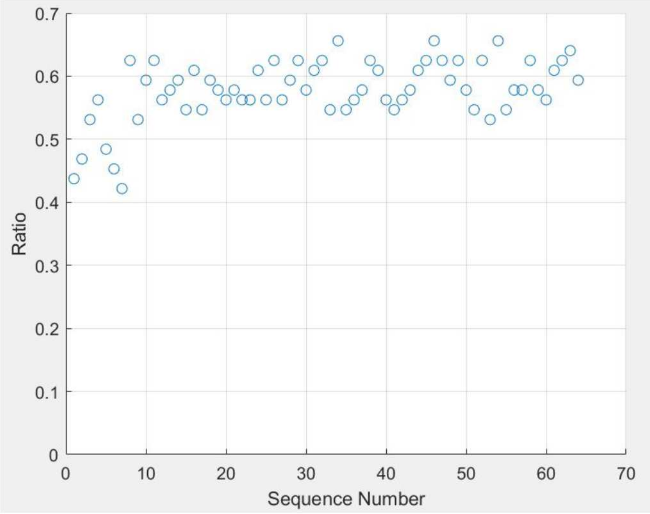

Fig. 7: Avalanche effect analysis for last round

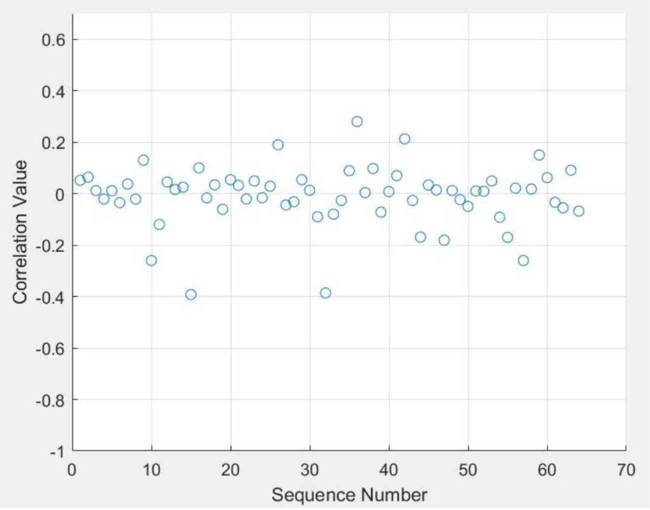

Fig. 8: Correlation Coefficient of Proposed Encryption Technique

The proposed encryption algorithm is secured as compared to the other algorithm, which is analyzed by the avalanche effect and correlation coefficient. This could be because of the following reason. Firstly, while de-mutation, the correct information about the bit is necessary, which would be challenging to crack. Secondly, a cross-over pattern would be impossible to hack. Thirdly, the extra secret key, without that, nothing is possible. So, the proposed encryption algorithm is more secure than any other algorithm with reasonable throughput and encryption time.

VI. Conclusion

UAV use is steadily growing in areas where it is difficult or unsafe for humans to accomplish tasks directly as aviation technology progresses. However, unauthorised and hostile attacks against UAVs have occurred because of the security flaws in UAVs. Therefore, for transmitting the data of drone's securely from the BS to the IoT cloud to provide the access to the far distance BS, encryption and decryption algorithms are proposed. So, the proposed cryptographic algorithm could be preferred for more security.

REFERENCES

[1] H. Wang, H. Cheng, and H. Hao, "The Use of Unmanned Aerial Vehicle in Military Operations," *Long S., Dhillon B.S. (eds) Man-Machine-Environment System Engineering, MMESE, Lecture Notes in Electrical Engineering*, vol. 645, Springer, Singapore, 2020.

[2] Y. Li, C. Pu, "Lightweight digital signature solution to defend micro aerial vehicles against man-in-the-middle attack," *In 2020 IEEE 23rd international conference on computational science and engineering (CSE)*, pp. 92-97, 2020.

[3] E. Vattapparamban, I. Güvenç, AI. Yurekli, K. Akkaya, S. Uluağaç, "Drones for smart cities: Issues in cybersecurity, privacy, and public safety," *In 2016 international wireless communications and mobile computing conference (IWCMC)*, pp. 216-221, 2016.

[4] A. Toma, N. Cecchinato, C. Drioli, G.L. Foresti, G. Ferrin, "Towards drone recognition and localization from flying UAVs through processing of multi-channel acoustic and radio frequency signals: a deep learning approach," *In: IST-190 Symposium on AI, ML and BD for Hybrid Military Operations (AI4HMO)*, 2021.

[5] E. Yanmaz, S. Yahyanejad, B. Rinner, H. Hellwagner, C. Bettstetter, "Drone networks: Communications, coordination, and sensing," *Ad Hoc Networks*, vol. 68, pp. 1–15, 2018.

[6] R. Muzaffar, E. Yanmaz, C. Raffelsberger, C. Bettstetter, A. Cavallaro, "Live multicast video streaming from drones: an experimental study," *Autonomous Robots*, vol. 44, pp. 75–91, 2020.

[7] M. Rana, Q. Mamun, R. Islam, "Lightweight cryptography in IoT networks: A survey," *Future Generation Computer Systems*, vol. 129, pp. 77-89, 2022.

[8] R. B. Abduljabbar, O. K. Hamid, N. J. Alhyani, "Features of genetic algorithm for plain text encryption," *International Journal of Electrical and Computer Engineering*, vol. 11, no. 1, pp. 434, 2021.

[9] A. Alabaichi, F. Ahmad, R. Mahmod, "Security analysis of blowfish algorithm," *Second International Conference on Informatics & Applications (ICIA)*, pp. 12-18, 2013.