Hindawi
Wireless Communications and Mobile Computing
Volume 2023, Article ID 9787984, 1 page
https://doi.org/10.1155/2023/9787984

Retraction

Retracted: Transformation Path of Modern Media from the Perspective of Internet of Things

Wireless Communications and Mobile Computing

Received 8 August 2023; Accepted 8 August 2023; Published 9 August 2023

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope
(2) Discrepancies in the description of the research reported
(3) Discrepancies between the availability of data and the research described
(4) Inappropriate citations
(5) Incoherent, meaningless and/or irrelevant content included in the article
(6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] Y. Zhang, M. A. I. Yasin, S. A. B. S. Alsagoff, and A. L. Hoon, "Transformation Path of Modern Media from the Perspective of Internet of Things," *Wireless Communications and Mobile Computing*, vol. 2022, Article ID 1556549, 13 pages, 2022.

Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 1556549, 13 pages
https://doi.org/10.1155/2022/1556549

Research Article

Transformation Path of Modern Media from the Perspective of Internet of Things

Yujie Zhang,[1,2] Megat Al Imran Yasin,[1] Syed Agil Bin Shekh Alsagoff,[1] and Ang Lay Hoon[3]

[1]*Department of Communication, FBMK University Putra Malaysia, Malaysia*
[2]*Guangxi Normal University, School of Design, China*
[3]*Department of Foreign Languages, FBMK University Putra Malaysia, Malaysia*

Correspondence should be addressed to Megat Al Imran Yasin; gs54800@student.upm.edu.my

Received 27 June 2022; Revised 14 July 2022; Accepted 26 July 2022; Published 22 August 2022

Academic Editor: Kuruva Lakshmanna

The Internet of Things (IoT) is a new technology revolution that aims to link all ordinary physical items to the Internet, creating a massive worldwide network of uniquely connected things that can exchange information and fulfill planned activities, resulting in considerable advantages for consumers. Researchers have started to explore new techniques of technical help in various fields (e.g. health, transport, and education) as the Internet of Things has grown in popularity in recent years. In this research, we present a revolutionary IoT paradigm with an encryption mechanism to establish a kind of network that would allow the more intelligent media-data transfer. Initially, we collected COVID-19-related data and preprocessed the raw data using the median absolute deviation method. The preprocessed data that is to be transferred to the media is then stored in the IoT device using various sensors. To improve the security of the data, we propose Robust Modern Media Data Encryption (RMMDE) algorithm with Enhance Cuckoo Swarm Optimization (ECSO) algorithm. The suggested mechanism is compared to the traditional encryption approaches, and the metrics are evaluated using the OriginPro tool. This proposed methodology could be a start point for better and more efficient media data transmission.

1. Introduction

The development of new communication technologies is largely responsible for the tremendous shifts in lifestyle that have taken place over the last century. [1] Traditional media include "books," "periodicals," "newspapers," "TV," "radio," "cinema," and "music." Traditional media includes all forms of communication before the Internet and modern media. Modern media include "video games," "the Internet," and "social media" [2]. A comparison of people's attitudes about traditional and modern media is shown in Figure 1. Everyone's life has been transformed by the media. It is an important part of modern life. Currently, it is used as food to either help or hurt society.

The media has a huge impact on society. People can learn about a wide range of topics and establish their thoughts and judgments on a variety of topics due to the mainstream media. The media keeps people up-to-date on local and global events. Media is frequently called a "mirror" of contemporary society, yet it influences our everyday lives [3, 4].

Both society and culture are influenced by media. The media systems in place in many countries are shaped by the laws that govern them. Society is shaped and structured by various forms of communication, including messages sent through the media. Our perspectives are often influenced by the ever-changing and expanding media in today's culture. Recognition of cultural differences in moral standards and the need to halt such acts regardless of whether or not they are tolerated in other countries is critical to the preservation of human dignity. The link between culture and new media is fraught with complications and challenges. The apprehension that Plato had regarding the impact of new media on culture is still relevant to the discussion that is taking place now over the impact of the Internet and social

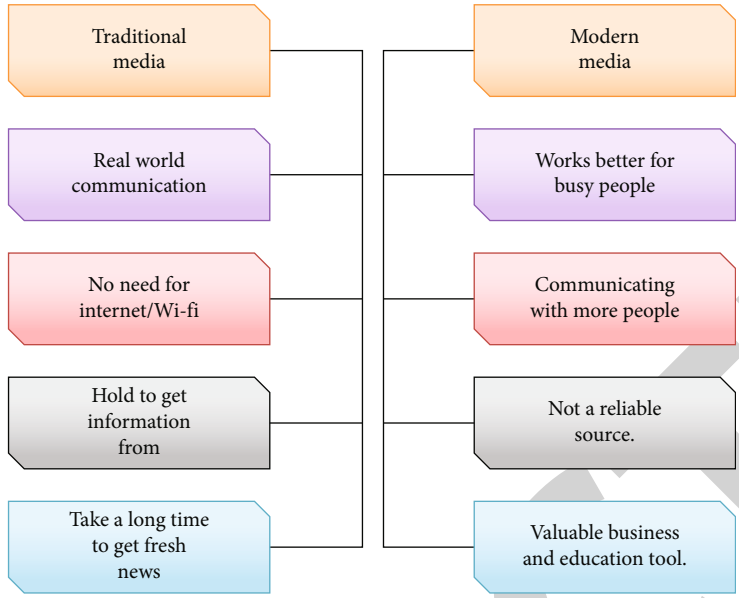

Figure 1: Tradition media vs. modern media.

media [5]. Concerns regarding the effect that social media use has on young people's cognitive development readily mix and mingle with hyperbolic stories of malicious hackers, internet trolls, identity theft, and other online crimes. The Internet is used here as a metaphor for greater social and cultural fears, and it does so through communicating these anxieties.

It becomes a common knowledge that the Internet is reshaping human existence in a positive direction toward a more awakened and creative state. Big data and the IoT, we are told, are about to revolutionize our way of life. The IoT is being used to describe the connectivity of things as "a system of uniquely identifiable and connected constituents (termed as Internet-connected constituents) capable of virtual representation and virtual accessibility leading to an Internet-like structure for remote locating, sensing, and/or operating the constituents with real-time data/information flows between them". Common day-to-day things have developed over the past five years, frequently through communication between sensors and control systems, to incorporate new capabilities [6]. Every day, the Internet of Things (IoT) becomes more and more pervasive in the lives of ordinary people. Figure 2 depicts the applications of IoT. Transferring pandemic news through IoT has rapidly increased in China. Several security issues, such as the transmission of fake news related to COVID19, media data privacy, and so on, arise when transferring media data via IoT. Hence, we present a revolutionary IoT paradigm with an encryption mechanism to establish a kind of network that would allow more intelligent and secured media-data transfer.

The paper's contribution is presented in the following points:

(i) The suggested work is based on the transformation path of modern media from an IoT perspective

(ii) The process is carried out by collecting COVID-19 datasets

(iii) Then the collected raw data are transformed into an understandable format by using the median and median absolute deviation method

(iv) Then to improve the security of the data, we propose Robust Modern Media Data Encryption (RMMDE) algorithm with Enhance Cuckoo Swarm Optimization (ECSO) algorithm

The remaining part of the study is depicted as Section 2 includes a literature survey, Section 3 displays the suggested work, Section 4 shows the performance analysis, and Section 5 concludes the research with a summary of the findings.

2. Literature Survey

From the vantage point of the Internet of Things, numerous authors have produced works that discuss the evolution of the modern media landscape. This section depicted a few of the featured masterpieces.

In [7, 8] the author depicts that the data they gathered from Chinese news organizations were used to increase "security," "team collaboration," "high-speed network access," and "public accessibility." As a means of putting IoT adoption into context, we employed the "Rivest-Shamir-Adleman (RSA)" encryption and the "Hybridized Fruitfly Bumblebee Optimization Algorithm (HFBOA)" to optimize the process. Security of news data, team communication, and implementation costs are the three key issues facing the news industry today. The performance of the proposed method is evaluated in comparison to other methods. A comparison of WSN and NB-networking IoT's topology and fusion technologies are made in [9]. The conventional wireless sensor network's coverage mechanism is then

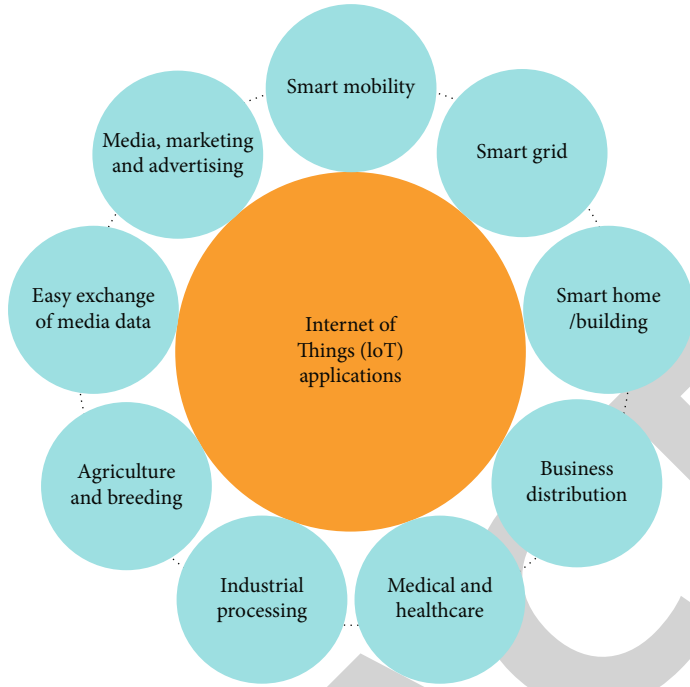

Figure 2: Applications of IoT.

described. The old approach had poor node connection and little coverage from not searching subgroup nodes locally. The node redeployment method of wireless sensor network based on the frog hopping algorithm combines local subgroup search and global information exchange. This method abandons CIS and utilizes B/S and Java Web to build a web-based system. Several issues, including poor node connectivity and low coverage brought on by not conducting a local search of subgroup nodes, are suggested. The author of [10, 11] discusses several applications of the IoT that play an important part in the lives of human beings on a day-to-day basis. The Internet of Things has produced important advancements that have elevated human existence to a higher level. The user may obtain the information from a faraway due to this technology. Using IoT and mobile technologies, the author of [12, 13] proposes a "learning media repository and delivery system (LMRD)." Its goal was to aid in the implementation of a hands-on teaching approach. Students can use their mobile devices to sketch, edit, or contribute comments to learning media or course materials that the teacher broadcasts directly to the devices of their students. The students can then broadcast back their comments or edits to convey or reflect their ideas. A Raspberry Pi 3B+ server and two mobile devices make up the model. To accommodate the majority of mobile platforms, the mobile applications were developed utilizing a cross-platform approach. The three dimensions of the examination were usability, functionality, and security.

In [14, 15] the author offers a novel privacy-preserving social media 3.0 paradigm that displays SM and IoT interaction and forecasts how it could affect user behavior. The framework has 3 parts. First, SM-IoT, a novel relational dataset, connects users dynamically to IoT services and processes data heterogeneity. Second, a preprocessing module filters heterogeneous data and preserves privacy. Third, data analytics is used to assess data complexity and determine user behavior. Despite the growth of SM datasets, current benchmarks do not fit collaborative machine learning-enabled privacy-preserving algorithms and recommender systems. This makes it harder to compare and develop alternative structures, which is vital for improving privacy frameworks and recommendation algorithms. Two well-known IoT session protocols, the "Constrained Application Protocol (CoAP)" and the "Message Queuing Telemetry Transmission Sensor Network Protocol (MQTT-SN)", are investigated in [16, 17] to enable efficient media transport over LLNs. By comparing CoAP and MQTT-SN to the classic RTP, which is studied, modeled, and compared to the old RTP, an effective RTC solution for embedded IoT devices is described and specified. In [18], the author discusses IoT, big data, its importance, data sources, big data applications, IoT architecture and security concerns, IoT standards and protocols, single points of failure, IoT code, etc. In [19] the author illustrates that IoT-based media distribution is the focus of this research, which presents a unique intelligent media distribution system. "UPnP," "face recognition," "intelligent human-machine interface," and "family database technologies" are all integrated into this system's design. HNDs compatible with UPnP is possible for network devices to discover one other through the use of UPnP. Incorporating face recognition, UPnP networked devices can detect the operational user in front of them. The intelligent human-machine interface in a home network lets a user compel any media content to be distributed or displayed on the UPnP-based device nearby the user as the user moves across the network. A prototype and an actual demonstration of

UPnP-based network devices in home networks are also shown in their study. In [20], the author describes IoT network architecture and security problems and reviews media data protection in "wireless sensor networks (WSNs)." Next, we will present "Efficient Algorithm for Media-based Surveillance System (EAMSuS)" in an IoT network for the Smart City Framework. It combines two methodologies for WSN packet routing and safety introduced by other researchers while reclaiming the new media compression standard, "High-Efficiency Video Coding (HEVC)". IoT and "Cloud Computing (CC)" has led to new technological support strategies in various industries. Coverage factor, predicted event score, dependability ratio, error impact, and energy use in the sensing node rely on average node timings in WSN for power-sharing and processing of communication networks, principally information exchange. This article examines several technologies to develop a smarter media-data transport network. Open source CC analyzers and simulators have been researched. These technologies study data collecting, storage, administration, processing, and analysis. The experiments used Eclipse-based CloudSim. Following CloudSim's network performance measurements, we employ the Contiki OS Cooja emulator to validate and obtain further metrics [21]. Media data should be encrypted before storage in light of the security risk. Due to their inability to modify their speed to match the throughput fluctuation of media data in real-time RPS, conventional full encryption, and partial encryption techniques are not suited to RPS. To improve the security of the data, we propose Robust Modern Media Data Encryption (RMMDE) algorithm with Enhance Cuckoo Swarm Optimization (ECSO) algorithm.

2.1. Problem Statement. The COVID-19 outbreak is a grave emergency, and official government agencies such as the National Health Commission are often cited as data sources in pertinent news articles. This is notably seen in statistics and news stories depicting the epidemic's shifting pattern. Within the setting of the pandemic, the media formed in search of disease-related information. False news posing as established illness prevention and control measures caused an excess of deception. This process interfered with people's behavior and health. As a result, our study proposes an effective security paradigm for modern media to address the aforementioned challenges.

3. Proposed Methodology

The transformation route of modern media from the perspective of the Internet of Things is studied thoroughly in this section. Figure 3 displays the proposed technique's overall flow. Mainstream media broadcast news and public opinion propaganda, and its content may reflect popular attitudes during an epidemic. The media reports China's antiepidemic effort. The reports from this period may serve as research objects and lead to more objective and precise conclusions. Hence, initially COVID-19 case report of China was gathered. To minimize the concerns of privacy leakage, fake news, copyright protection, etc., we present a novel approach called the Robust Modern Media Data Encryption method, and to optimize the process, we utilize the Cuckoo Swarm Optimization method.

3.1. Dataset Collection. According to the White Paper "China's Action to Fight the New Coronary Pneumonia Epidemic," from January 20 to May 31, China's antiepidemic operations experienced four important stages: "containment of the spread of the epidemic," "the number of new local cases gradually decreased to single digits," "achieved decisive results in the defense of Wuhan and Hubei," and "national epidemic prevention and control has entered normalization."

After then, there was a minor rise in instances in several locations, especially in Beijing's June 11 notifications. Beijing reached "zero" new cases on July 19. This study spans from January 22, 2020, the eve of Wuhan's lockdown, through October 26, 2020, when the final epidemic-related data news was posted on Xinhua Net. [22]. Table 1 depicts the dataset features.

3.2. Preprocessing Using Median and Median Absolute Deviation. Raw datasets are anticipated to include missing values, aberrations, inaccurate recording, and insufficient sampling. Noise, missing numbers, and inconsistencies may all be found in raw data. The outcomes of data mining are affected by the quality of the data. Raw data is preprocessed to increase mining efficiency and convenience while also helping to enhance the quality of the data and, as a consequence, the mining results. There are several important aspects to consider when it comes to data mining, and one of the most significant is preprocessing. Data normalization is one of the preprocessing procedures utilized in most data mining systems. Before being given to any machine learning algorithm, the primary purpose of data normalization is to ensure the accuracy of the data. It is possible to do a variety of data normalizations. Scaling the data in the same range of values for each input feature helps decrease the neural network's bias toward one feature over another. Through the use of data normalization, the training time for each feature may be reduced. Modeling applications in which the inputs are typically on a broad range of scales may benefit from this. Rules such as Z-score, Min-Max, decimal scaling, and median normalization may be used for various procedures. As a starting point, we will look at the median and the median absolute deviation. The average distance between each data value and the mean is known as the mean absolute deviation (MAD) of a data collection. A measure of variance in data collection is the mean absolute deviation. We may determine how "spread out" the values in a data collection are by looking at the mean absolute deviation.

3.2.1. Median Absolute Deviation. Data variability in a univariate sample is well-captured by the median absolute deviation (MAD). In a COVID-19 media data collection, MAD is a statistical dispersion metric that is more resistant to outliers than the standard deviation. Computed values are used

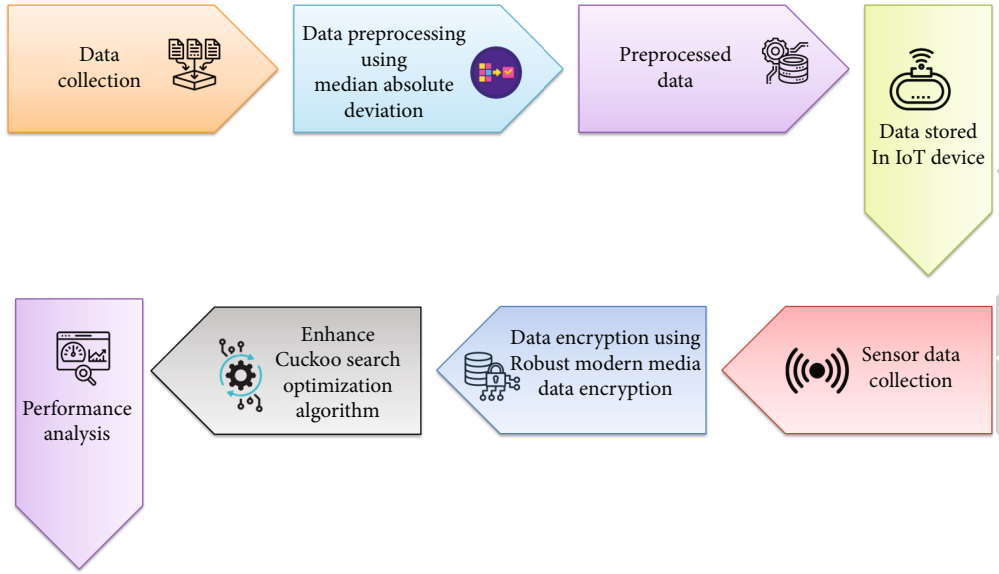

Figure 3: Flow of the proposed method.

Table 1: Dataset features.

Parts	Description
Production methods	Data analysis, digital expression
Production content	Descriptive words, data sources, subject, and scope of the topic
Visual design	Interactive design, infographic application, visual elements

to normalize the media data value of attribute I:

$$\hat{i} = \frac{i - \text{median}(i)}{\text{MAD}}, \tag{1}$$

where MAD = median $((\text{abs}(\{\text{id}\} - \text{median}(I)))$.

The integrated management solution identifies COVID news, which is reported by the Internet of Things security portal. This portal also provides real-time news dissemination, as well as accurate and wrong status. Terminal intrusion detection and dissemination are both prevented as a result of this when paired with the IoT gateway's ability to isolate the corporate network and perform baseline detection. The IoT technology is used to monitor a variety of processes, including the functioning of energy systems, economic usage, social utility, and other concerns. IoT-based data transfer connectivity can improve the data quality, reduce data gathering costs, and expand data service while attempting to minimize (or maximize) the loss function by upgrading and estimating network aspects that influence prototype learning and design output to approximate or attain the optimum solution, thus minimizing (or maximizing) the loss function. Preprocessed data is stored in IoT devices. In IoT data collection, sensors monitor Internet-connected devices. The sensors gather and deliver COVID-19 media data to monitor the IoT network's status [23].

3.3. Data Encryption Using Robust Modern Media Data Encryption (RMMDE). Media data of variable length and other compression techniques remove unneeded information from the original COVID-19 media data, resulting in compressed media content having drastically different statistical properties than uncompressed textual data. The byte-level unpredictability of the encoded data was found to be very high, according to the results of the analysis. We extend this statistical characteristic of standard video encryption strategy to a novel strategy that utilizes conventional block cypher to encrypt data (phase I) and utilizes its plaintext as the "stream cypher key" to encode another section of data (phase II). By altering the ratio between phases I and II, the speed of the encryption process may be changed.

In the first step of the fundamental method, the plaintext is cut up into substrings that are of the same length. In the second step of the encryption process, a standard block cypher algorithm is chosen and applied to one segment of media data. Thirdly, for the next l-blocks' stream cypher key, utilize the plaintext of the segment that came before it. The following stages make up the fundamental algorithm, which is based on the premise that the media data are stored in a FIFO buffer. The stages that make up the fundamental RMMDE algorithm are laid forth in Algorithm 1. This technique was developed for use with media files, as opposed to the real-time packets used by recording and playback systems. The robust method for encrypting modern media data is shown in Figure 4.

Start:
(1) The byte stream in the FIFO buffer is split into Seg Length segments by permuting and dividing it.
(2) Encode the initial n-segments using the standard block cypher method F.
Continue until you reach the last section:
(3) Encrypt the buffer's first segment, Seg_S using algorithm F.
(4) Its ciphertext is $Gseg_s = Seg_{s-1} \oplus Sef_s$ for the following o blocks.
(5) Repeat steps (3) and (4).
End Do
(6) Fill the final phase using Figure 7's filling approach, then encrypt it with B.
Stop

Algorithm 1: The basic RMMDE algorithm.

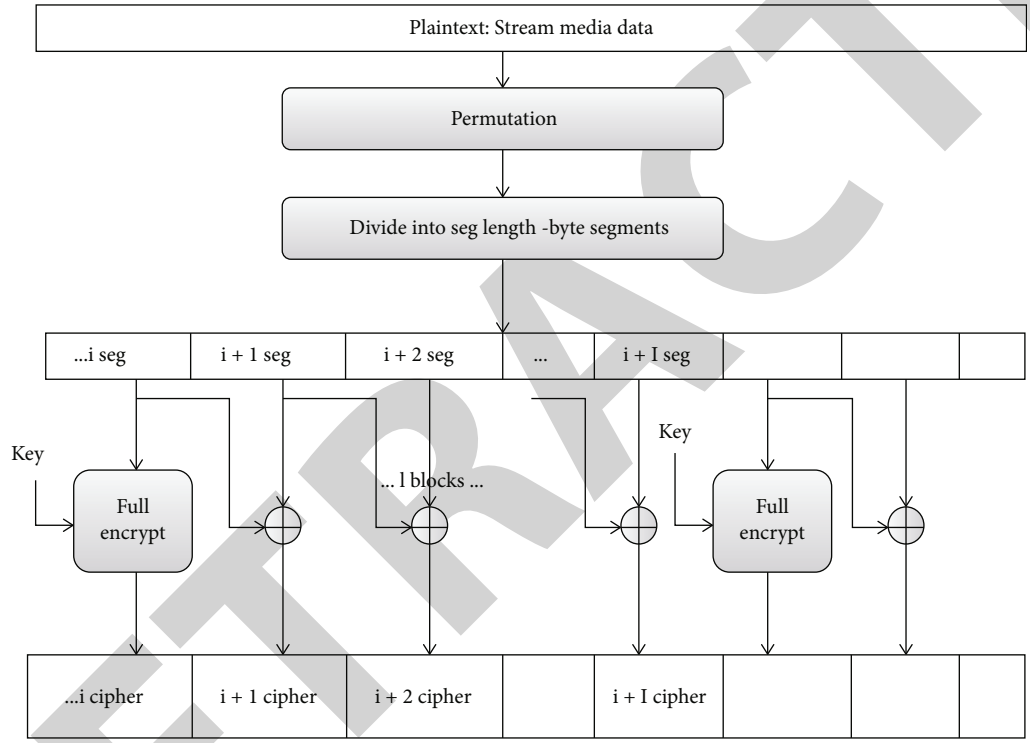

Figure 4: Framework of Robust Modern Media Data Encryption approach.

The first n-segments of the file are fully encrypted to prevent the attackers from guessing the file header; n is computed using the session key. To regulate encryption algorithm performance, the encryption speed parameter may be used. Either in a separate document or the header of each segment of the file, this parameter should be appropriately preserved for file encryption.

According to EF, the decryption process may decide the decryption method. The processes involved in the decryption procedure are shown in Algorithm 2. Because most conventional encryption techniques need the plain-block length to be split by a certain integer, in this situation, the value to be filled is the length of the filled bytes. Figure 5 shows two $n = 8$ cases.

$$\text{FillingLength} = q - (\text{Lengthmod}q), \tag{2}$$

$$\text{FillingValue} = q - (L\text{engthmod}q). \tag{3}$$

If EF is fully encrypted then
$PTB^{-1}(Clipher_a)$; // PlainText-PT
Else
$PlainText_a = PlainText_{a-1} \oplus Clipher_{a-1}$.
End

Algorithm 2: The decryption process.

3.3.1. Improved Algorithm for RTP Packets. The first technique, which was developed for byte stream, is an excellent choice for encrypting huge media files since it was created for byte stream. As a result of the fact that the recording and playback operations in Admire RPS operate on RTP packets, an algorithm that is based on packets is capable of achieving better levels of efficiency [24]. As a result, we

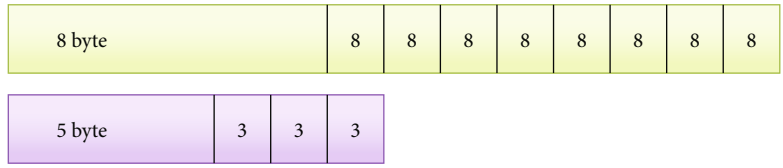

Figure 5: Rear padding in RMMDE.

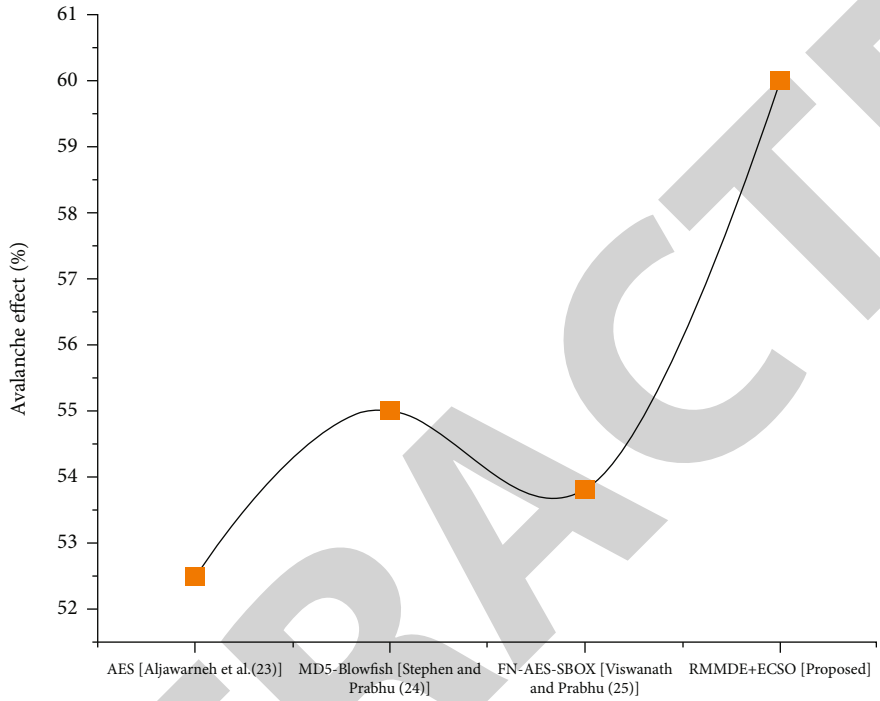

Figure 6: Avalanche effect of various encryption techniques.

develop a better method that is based on packets, as will be illustrated below. The value of the block header's one bit EF may be determined via

$$EF = \begin{cases} 1, & \text{ifpacketisfullyencrypted,} \\ 0, & \text{ifXorwiththepreviouspacket.} \end{cases} \quad (4)$$

The X or operator is implemented as Equation (3) since consecutive packets might have different lengths. In this equation, h_s^a is the sth byte of the packet a, g_s^a is the ciphertext of packet a, and PL^a is the length of packet a. That is to say, copy the previous packet and append it to the end of the current one if the current packet is longer than the previous one. One such illustration may be seen in Figure 6, in which PL^{i-1} equals 1000 and PL^i equals 1005.

$$g_s^a = h_s^a \oplus h_{smodPL^{a-1}}^{a-1}. \quad (5)$$

3.3.2. Adaptive-Speed Control Mechanism. While the input throughput and upper limit of the projected queuing time are reported in this section, the parameter regarding encryption speed control "l" in RMMDE is calculated using a speed control approach. To buffer the incoming data, RP server makes use of a FIFO queue. While the encryption process is taking place, fresh packets are added to the device's back, where they are stored until needed. In a video conference, the amount of media data may fluctuate considerably; thus, the speed control system should guarantee that the queuing delay is steady and under control while also making maximum use of encryption recourse [25].

We continue based on the following assumption to assess the nature of the link that exists between the input media data bandwidth, the queuing delay, and the encryption throughput: (1) media data packets arrive in a—Poisson distribution; (2) encryption capability is C; (3) maximum media data packet length, designated by O packet, is a restriction; and (4) memory is substantially bigger than the maximum packet length. The model shown here is that of a traditional M/M/1/K queuing system. Then, the average queuing latency k_{queue} is

$$k_{\mathrm{queue}} = \frac{1}{\mu - \lambda} * \frac{1 - (D+1)\rho^d + D_{\rho^{d+1}}}{1 - \rho^{d+1}}, \quad (6)$$

where $\mu = \mathrm{G}/O_{\mathrm{packet}}$ represents the number of packets an algorithm can encrypt in a given unit of time, $\rho = \lambda/\mu$ represents the load rate, and λ represents the rate at which packets arrive. If we suppose that the main memory capacity

Begin:
(1) Encrypt the initial q-packets by using the tried-and-true block cypher algorithm B.
Do
(1) Initial media data packets in buffer are encrypted
(2) Assume its ciphertext as $GPacket_s = Packet_{s-1} \oplus Packet_s$. for the next l packets of media data
(3) Repeat stages (3) to (4).
(4) End Do
(5) The final packet of media data is encrypted
End

Algorithm 3: The improved encryption algorithm.

Objective function $f(z), z = (z_1, z_2 \cdots \cdots . z_k)^V$
Create a starting p of n host nests $za(a = 1, 2, \cdots q)$
//p denotes population
While (v < Max Generation) or (stop criteria)
Get a cuckoo (say a) randomly;
Calculate quality/fitness B_a ;
Randomly pick a nest from n (say j);
Calculate quality/fitness B_s ;
If $(B_a > B_a)$
Swap j by the best solution;
End
A fraction of$H(H_i)$of worse nests are eliminated and the best ones are built at new locations;
Retain the most effective solutions;
Make a list of all of the solutions and choose the best one currently available;
End while
Post-processing

Algorithm 4: Cuckoo search optimization.

of RP server is much more than the length of a packet, then the value of the parameter D is becoming closer and closer to infinity, and we can derive the following equation from it:

$$\lim_{d \longrightarrow \infty} k_{\text{queue}} = \frac{1}{\mu - \lambda}, \quad \mu = \frac{1}{k_{\text{queue}}} + \lambda, \tag{7}$$

$$G = O_{\text{packet}} \left(\frac{1}{k_{\text{queue}}} + \lambda \right). \tag{8}$$

Therefore, given an upper limit of the anticipated queuing delay $k'_{\text{queue}} (k'_{\text{queue}} > 1/\mu)$, the minimum encryption speed G' should meet.

$$G' \geq \left(\left(\frac{1}{k'_{\text{queue}}} \right) + \lambda \right) * O_{\text{packet}}. \tag{9}$$

We can determine the minimal throughput that RMMDE can achieve with a restricted amount of queuing time by using Equation (9). In addition, if the quantity of queued media data packets surpasses a gate valve, the RMMDE's throughput may be enhanced by including parameter l in the practical system. This is possible when the gate valve is reached. The stages that make up the new and enhanced encryption technique are laid forth in Algorithm 3.

3.3.3. Enhanced Cuckoo Search Optimization (ECSO) Algorithm. The CS algorithm is an illustration of a naturally-inspired algorithm that was built based on the reproduction of cuckoo birds. It is essential, while working with CS algorithms, to compare alternative answers using cuckoo eggs. Cuckoos have a habit of placing their fertilized eggs in the nests of other cuckoos with the expectation that the offspring of these eggs would be nurtured by other cuckoos. When the cuckoos realize that the eggs in their nests do not belong to them, they will either remove the foreign eggs from the nest or they will quit the nest altogether. When this occurs, the cuckoos will either leave the nests entirely. Because it maintains a balance between a local random walk and a global random walk, the Cuckoo search algorithm is extremely useful at solving issues relating to the optimization of encryption. The switching parameter P_i ϵ[0,1] determines how much weight is given to local vs. global random walks in the overall evaluation. Equations (10) and (11), respectively, are used to define the local and global random walks in this context. Algorithm 4 is a concise

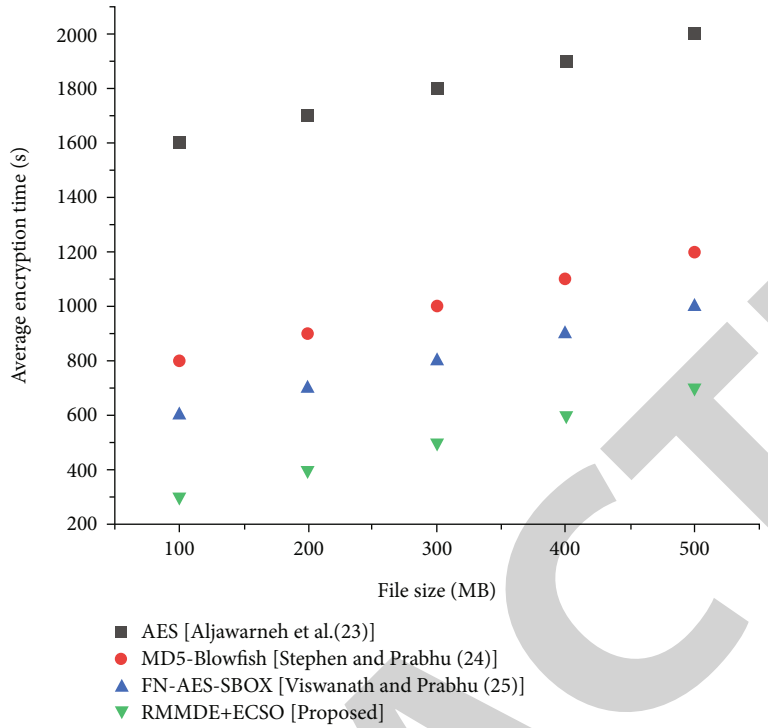

Figure 7: Media content file size versus encryption time.

way to describe the fundamental phases of the Cuckoo search algorithm, which are determined by three principles.

$$z_a^{v+1} = z_a^v + \alpha j \otimes (P_i - \varepsilon) \otimes (z_s^v - z_d^v), \tag{10}$$

$$z_a^{v+1} = z_a^v + \alpha O(j, \lambda). \tag{11}$$

There are three suggested CS algorithms for ECSO, all of which are based on dynamic switching parameters that grow in value as the number of CS iterations rises. Equations (12) through (14) serve as the basis for the definition of the ECSO algorithms. The first proposal for a CS algorithm makes use of a switching parameter, the value of which rises linearly in proportion to the number of CS iterations. Equation (12) defines the switching parameter.

$$h_{iGA} = (h_{i\mathrm{Max}})^* \left(\frac{G_a}{V_a}\right). \tag{12}$$

When the number of repetitions becomes up, the switching parameter in Equation (13) grows exponentially.

$$h_{iGA} = (h_{i\mathrm{Max}})^* \mathrm{Exp}\left(\frac{G_a}{V_a}\right). \tag{13}$$

Increasing the number of repetitions raises the power of three of the switching parameter in Equation (14).

$$h_{i\mathrm{GA}} = (h_{i\mathrm{Max}})^* \left(\frac{G_a}{V_a}\right)^3, \tag{14}$$

where $h_{i\mathrm{GA}}$ denotes iteration's parameter swap, $h_{i\mathrm{Max}}$ denotes switching parameter's maximum value, G_a denotes present iteration, V_a denotes Set a total number of iterations.

4. Results and Discussion

The major focus of this research is to protect the COVID-19 news content in the IoT network from malicious attackers. COVID-19 case report data is unprocessed raw data. The dataset's repeated case report about COVID-19 is removed and processed using data normalization to provide normalized data. In this paper, we proposed a novel RMMDE strategy optimized by ECSO to secure sensitive media information. The performance of RMMDE +ECSO was compared to the conventional encryption techniques in the privacy-preserving process of media contents. The existing techniques applied in this work for comparison are AES (Advanced Encryption Standard), FN-AES-SBox (Feistel network and AES with S-box), and MD5-Blowfish techniques. The indicators used for performance analysis are average encryption time, average decryption time, avalanche effect, average encryption and decryption throughputs, latency, reliability, and energy consumption.

Encryption time describes and specifies the average time used to encrypt input media content files. It is measured in seconds. When it comes to encryption, the amount of time it takes to encrypt a certain media data is directly proportional to the input media content file size. For encryption of media content file size of 500 MB, RMMDE+ECSO takes 700 s, AES takes 2000s, FN-AES-SBox takes 1000s, and MD5-Blowfish takes 1200s. Figure 7 shows that time taken

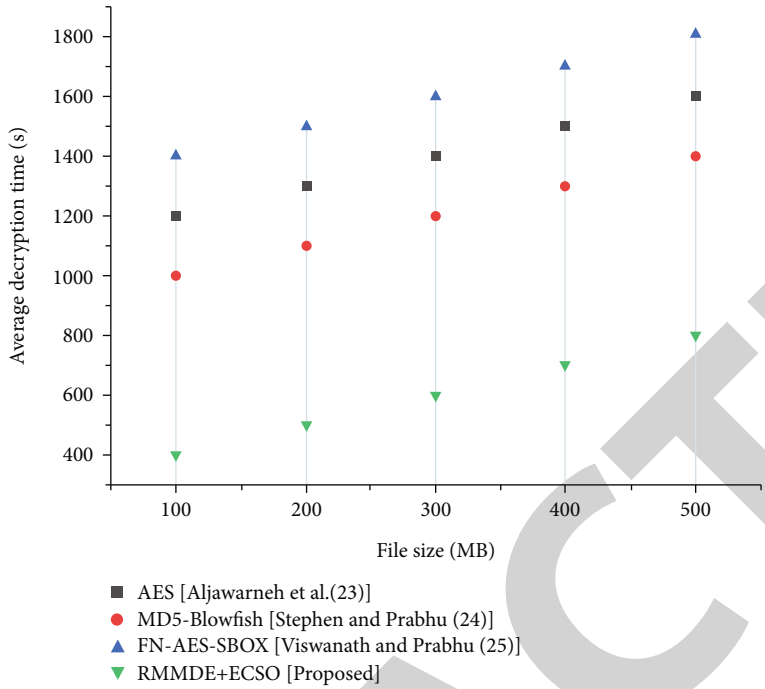

Figure 8: Media content file size versus decryption time.

by the proposed RMMDE+ECSO technique to encrypt the COVID-19 media information was lesser compared to existing approaches like AES, FN-AES-SBox, and MD5-Blowfish. This shows that the proposed technique fastly encrypts the media data which might be due to the optimization of RMMDE scheme by ECSO.

Average decryption time refers to the time consumed for converting encrypted COVID-19 media data into original media data. It is measured in seconds. For decrypting media content file size of 500 MB, RMMDE+ECSO takes 800 s, AES takes 1600s, FN-AES-SBox takes 1800s, and MD5-Blowfish takes 1400s. From Figure 8, it is observed that the proposed RMMDE+ECSO technique takes lesser time to decrypt the COVID-19 media information compared to existing approaches like AES, FN-AES-SBox, and MD5-Blowfish. This shows that RMMDE+ECSO technique quickly decrypts the COVID-19 media information whenever required for analysis.

One of the desired properties of any encryption scheme is the avalanche effect. A little change in the plain text or the key should cause a large change in the encrypted text. Avalanche effect is the name for this characteristic. The ability of proposed and conventional algorithms in ensuring the security of media data is examined using the avalanche effect.

$$\text{Avalanche effect} = \frac{\text{Quantity of modified bits in ciphertext}}{\text{Bits used in ciphertext}}. \tag{15}$$

It is calculated using the algorithm's strength, which is determined by how well it resists threats and real-time

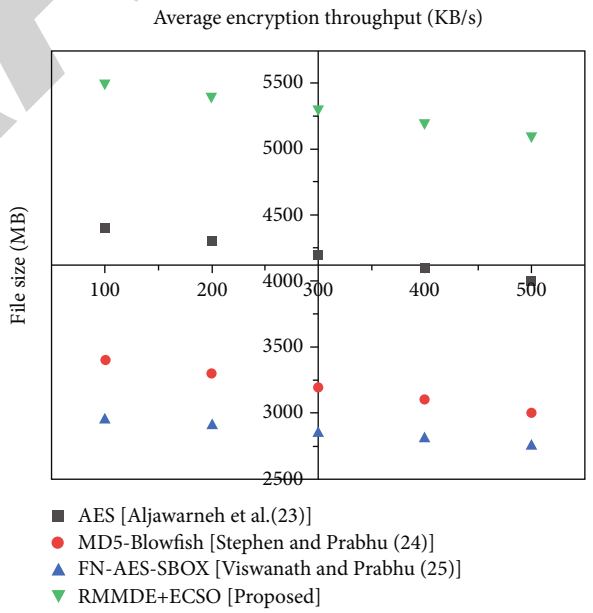

Figure 9: Media content file size versus average encryption throughput.

assaults in media data transmission. In encryption techniques, the avalanche effect is described as the ratio of modified bits in the cypher text to the total number of bits in the cypher text. When compared to the other benchmark techniques in Figure 6, the proposed method RMMDE+ECSO had the greatest avalanche impact. This depicts that RMMDE+ECSO resists the threats in media data transfer.

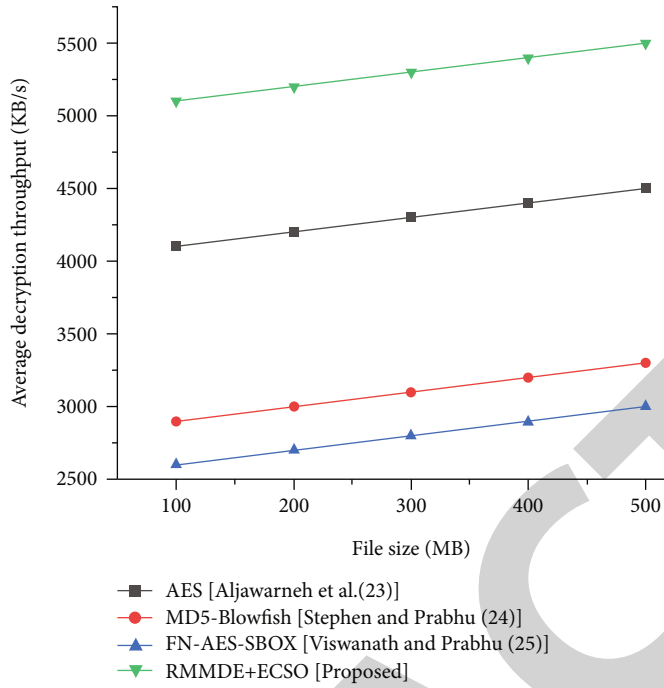

Figure 10: Media content file size versus average decryption throughput.

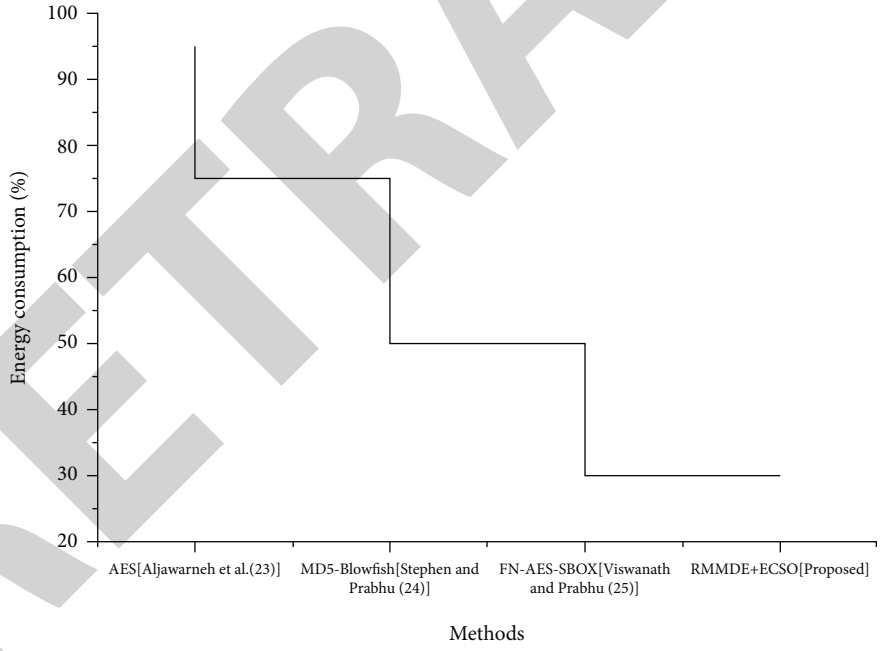

Figure 11: Energy consumption of various security models.

The average encryption throughput is calculated by the amount of data encrypted in unit time by the encryption approach. Figure 9 depicted that the encryption throughput of the proposed algorithm is superior to that of benchmark techniques like AES, FN-AES-SBox, and MD5-Blowfish. This showed that RMMDE strategy efficiently encrypts the COVID-19 media data.

The average decryption throughput is calculated by the amount of data decrypted in unit time by the algorithm. Figure 10 depicted that the decryption throughput of the proposed algorithm is superior to that of benchmark techniques like AES, FN-AES-SBox, and MD5-Blowfish. This showed that RMMDE strategy efficiently recovers the original COVID-19 media data whenever necessary for data analysis.

The amount of energy or power used for encryption of COVID-19 media data is referred to as energy consumption. As shown in Figure 11, the energy consumption of RMMDE

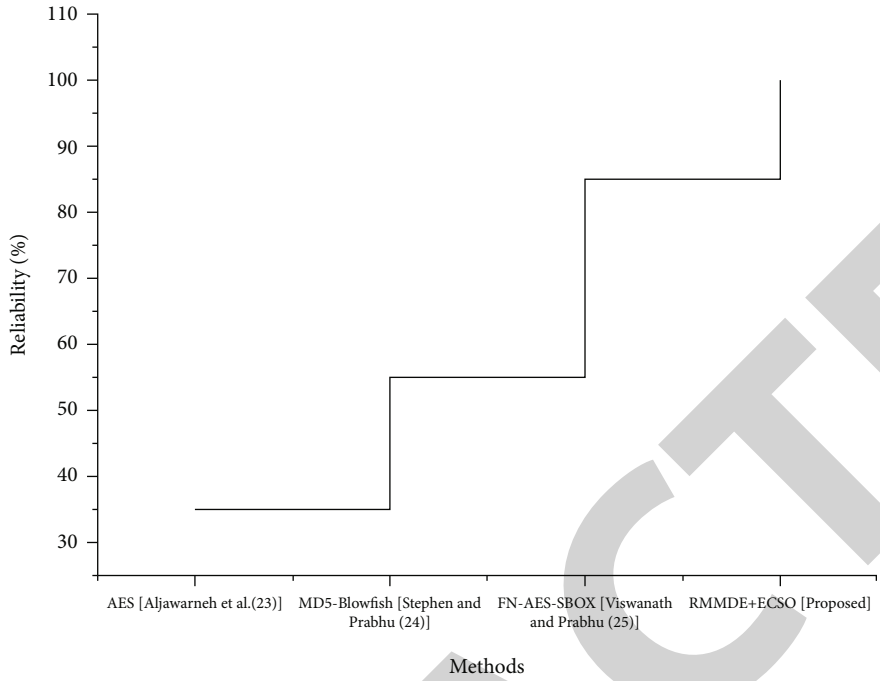

Figure 12: Comparative analysis of reliability of different security models.

+ECSO approach in processing media contents is lower than conventional strategies like AES, FN-AES-SBox, and MD5-Blowfish. This illustrates that RMMDE+ECSO is energy-efficient in encrypting media information.

The capacity of a security-enforcing algorithm to perform without fail in a given environment for a certain amount of time is referred to as reliability. The recommended solution was tested for its reliability to ensure the security of COVID-19 media data. The comparative analysis provided in Figure 12 shows that RMMDE+ECSO is more reliable than AES, FN-AES-SBox, and MD5-Blowfish.

As Internet technologies progress, a growing quantity of current media data is readily transmitted, saved, and shared across many social media and other platforms. Privacy difficulties, fake news generation, copyright protection, data tampering, and identity theft may arise as a result of sharing such contemporary media data through IoT. As a result, the preservation of such media data has piqued the interest of several research communities. To address these concerns, data encryption schemes have become more popular in recent years as a means of protecting media content by encrypting media data for eliminating fake media news. We have proposed RMMDE approach to secure COVID-19 media information in China and optimized the encryption process of RMMDE using ECSO. We compared the efficacy of the proposed technique in securing media data with benchmark schemes like AES, FN-AES-SBox, and MD5-Blowfish. Though the benchmark schemes show better encryption performance, they have some limitations which are described below. AES is very complex to implement in media data processing software taking both performance and security into consideration [26]. Each pair of users needs a unique key to decrypt the media data, so as the number of users increases; key management becomes complicated with MD5-Blowfish approach [27]. Though FN-AES-SBox exhibits higher data security, it consumes larger energy for data processing [28]. But our proposed approach RMMDE+ECSO secures the media data more efficiently compared to conventional schemes. In addition, it is energy-efficient and highly reliable in ensuring the security of COVID-19 media data.

5. Conclusion

The COVID-19 pandemic data news issued by Xinhua Net's data news section can track the outbreak's progress in real-time. The mainstream media acts as a front for news reporting and propaganda that is intended to shape public opinion, and the content of the mainstream media's report may reflect the trajectory that public opinion is headed in during an epidemic. As a result, it focuses the majority of its emphasis on the pattern of the pandemic. The safety of the data is the most significant obstacle that must be overcome in the modern media. In this paper, COVID-19-related data were gathered and preprocessed the raw data using the normalization method. The preprocessed data that is to be transferred to the media is then stored in the IoT device using various sensors. To improve the security of the data, we propose Robust Modern Media Data Encryption (RMMDE) algorithm with Enhance Cuckoo Swarm Optimization (ECSO) algorithm.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts 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.

References

[1] D. Croteau and W. Hoynes, *Media/Society: Technology, Industries, Content, and Users*, Sage Publications, New York, 2018.

[2] A. Enz, V. Schöffl, M. Simon, D. A. Back, T. Tischer, and C. Lutter, "Generation "social media": use of modern media to gain information regarding sports injuries," *Sportverletzung Sportschaden: Organ der Gesellschaft fur Orthopadisch-traumatologische Sportmedizin*, vol. 35, no. 2, pp. 95–102, 2021.

[3] A. Hill, *Media Experiences: Engaging with Drama and Reality Television*, Routledge, United Kingdom, 2018.

[4] H. Garg, "Digital twin technology: revolutionary to improve personalized healthcare," *Science Progress and Research (SPR)*, vol. 1, no. 1, pp. 32–34, 2021.

[5] A. I. Ismail and B. Uyuni, "Theology to technology the shift of facilities media Da'wa in millennial era," 2020.

[6] J. Chin, V. Callaghan, and S. B. Allouch, "The Internet-of-Things: reflections on the past, present and future from a user-centered and smart environment perspective," *Journal of Ambient Intelligence and Smart Environments*, vol. 11, no. 1, pp. 45–69, 2019.

[7] X. Wang, "The impact of IoT on news media in the smart age," *Mobile Information Systems*, vol. 2022, Article ID 2238233, 13 pages, 2022.

[8] Z. Li, "Treatment and technology of domestic sewage for improvement of rural environment in China-Jiangsu: a research," *Science Progress and Research (SPR)*, vol. 2, no. 1, 2022.

[9] Y. Sun, "Research on the method of digital media content creation based on the internet of things," *Computational Intelligence and Neuroscience*, vol. 2022, Article ID 8529875, 10 pages, 2022.

[10] M. S. Dawood, M. J. Margaret, and R. Devika, "Review on applications of internet of things (IoT)," *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, vol. 7, no. 12, 2018.

[11] S. O. Salihu and Z. Iyya, "Assessment of physicochemical parameters and organochlorine pesticide residues in selected vegetable farmlands soil in Zamfara State, Nigeria," *Science Progress and Research (SPR)*, vol. 2, no. 2, 2022.

[12] K. Saraubon, "Learning media repository and delivery system for smart classroom using IoT and mobile technologies," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 13, no. 2, 2019.

[13] A. Shahabaz and M. Afzal, "Implementation of high dose rate brachytherapy in cancer treatment," *Science Progress and Research*, vol. 1, no. 3, pp. 77–106, 2021.

[14] S. Salim, B. Turnbull, and N. Moustafa, "Data analytics of social media 3.0: privacy protection perspectives for integrating social media and Internet of Things (SM-IoT) systems," *Ad Hoc Networks*, vol. 128, article 102786, 2022.

[15] R. N. Mody and A. R. Bhoosreddy, "Multiple odontogenic keratocysts: a case report," *Annals of Dentistry*, vol. 54, no. 1-2, pp. 41–43, 1995.

[16] R. Herrero, "Analysis of IoT mechanisms for media streaming," *Internet of Things*, vol. 9, article 100168, 2020.

[17] B. Ahmed and A. Ali, "Usage of traditional Chinese medicine, western medicine and integrated Chinese-Western medicine for the treatment of allergic rhinitis," *Official Journal of the Zhende Research Group*, vol. 1, no. 1, pp. 1–9, 2020.

[18] S. B. B. Priyadarshini, A. Bhusan Bagjadab, and B. K. Mishra, "The role of IoT and big data in modern technological arena: a comprehensive study," in *Internet of things and big data analytics for smart generation*, pp. 13–25, Springer, Cham, 2019.

[19] C. L. Hu, H. T. Huang, C. L. Lin, N. H. M. Anh, Y. Y. Su, and P. C. Liu, "Design and implementation of media content sharing services in home-based iot networks," in *2013 international conference on parallel and distributed systems*, pp. 605–610, Seoul, Korea (South), December 2013.

[20] V. A. Memos, K. E. Psannis, Y. Ishibashi, B. G. Kim, and B. B. Gupta, "An efficient algorithm for media-based surveillance system (EAMSuS) in IoT smart city framework," *Future Generation Computer Systems*, vol. 83, pp. 619–628, 2018.

[21] C. Stergiou, K. E. Psannis, A. P. Plageras, Y. Ishibashi, and B. G. Kim, "Algorithms for efficient digital media transmission over IoT and cloud networking," 2018.

[22] J. Liu, "Visualization of data journalism of China's mainstream media in public health emergences: taking the data news section of Xinhua net as an example," *Journal of Physics: Conference Series*, vol. 1880, no. 1, article 012038, 2021.

[23] S. C. Nayak, B. B. Misra, and H. S. Behera, "Impact of data normalization on stock index forecasting," *International Journal of Computer Information Systems and Industrial Management Applications*, vol. 6, no. 2014, pp. 257–269, 2014.

[24] A. H. Hussein, M. Abu-Alhaija, and K. Nairoukh, "New RTP packet payload shrinking method to enhance bandwidth exploitation over RTP protocol," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 8, 2020.

[25] J. Wu, Y. Tian, P. Walker, and Y. Li, "Attenuation reference model based adaptive speed control tactic for automatic steering system," *Mechanical Systems and Signal Processing*, vol. 156, article 107631, 2021.

[26] S. Aljawarneh, M. B. Yassein, and W. A. A. Talafha, "A multithreaded programming approach for multimedia big data: encryption system," *Multimedia Tools and Applications*, vol. 77, no. 9, pp. 10997–11016, 2018.

[27] A. Stephen Dass and J. Prabhu, "Comparative analysis of a systematic coherent encryption scheme for large-scale data management using cryptographic encryption technique," in *Smart intelligent computing and applications*, pp. 427–437, Springer, Singapore, 2019.

[28] G. Viswanath and P. V. Krishna, "Hybrid encryption framework for securing big data storage in multi-cloud environment," *Evolutionary Intelligence*, vol. 14, no. 2, pp. 691–698, 2021.