Analysis of the Security of Internet of Multimedia Things in Wireless Environment

Nabeel Mahdy Haddad[1], Mustafa sabah Mustafa[2], Hayder Sabah Salih[3], Mustafa Musa Jaber[4,5,*] and Mohammed Hasan Ali[6]

[1]*College of Education, Misan University, Iraq*
[2]*Department of Computer Science, Dijlah University College, Baghdad, 10021, Iraq*
[3]*Department of Private Education in the Iraqi Ministry of Higher Education and Scientific Research, Baghdad, 10024, Iraq*
[4]*Department of Computer Science, Al-turath University College, Baghdad, 10021, Iraq*
[5]*Department of Medical Instruments Engineering Techniques, Al-farahidi University, Baghdad, Iraq*
[6]*Computer Techniques Engineering Department, Faculty of Information Technology, Imam Ja'afar Al-Sadiq University, Najaf 10023, Iraq*
E-mail: nabeel.mahdy@uomisan.edu.iq; mustafa.sabah@duc.edu.iq; haydersabah2@gmail.com; Mustafa.jaber@turath.edu.iq; mustafa_musajaber67@outlook.com; mh180250@gmail.com
[*]*Corresponding Author*

Received 09 December 2022; Accepted 24 April 2023;
Publication 05 December 2023

Abstract

The Internet of Things (IoT) and real-time flexibility improve people's lives, and IoT applications rely heavily on multimedia sensors and devices. An interconnected network of IoT multimedia devices has made the Internet of Medical Things (IoMT). It creates massive data distinct from what

Journal of Cyber Security and Mobility, Vol. 13_1, 161–192.
doi: 10.13052/jcsm2245-1439.1316

the Internet of Things (IoT) produced. Smart traffic monitoring and smart hospitals are only a few examples of real-time deployment applications. IoMT data and decision-making must be made quickly since it directly impacts human life. The security heterogeneity of optimization issues is a significant challenge for enabling multimedia applications on the IoT. The IoMT has difficulty achieving low-cost data collecting while maintaining data security. An Internet of Multimedia Things in a wireless environment (IoMT-WE) system decreases the bandwidth and privacy risk caused by the revocation list, ensures the integrity of batch verification information, and corresponds with Vehicular ad hoc network (VANET) security performance. The proposed method uses random subsampling and chaotic convolution to collect numerous images. The sampling method is safe since the measurement matrix is controlled by chaos. As part of the IoMT architecture, wireless multimedia sensor nodes can be more easily deployed over the long term for real-time multimedia. The Wireless Multimedia Sensor Network (WMSN) comprises nodes that can capture both multimedia and non-multimedia data. The ioMT-WE system has been tested and found to be secure and effective.

Keywords: Wireless environment, multimedia applications, internet of multimedia things, VANET, chaotic convolution, and sampling.

1 Overview of Security in a Wireless Environment

Internet of Things (IoT) technologies are swiftly created and widely applied as information technology progresses in the environment, transportation, medical care, agriculture, and other fields [1]. In the IoT, openness, and data sharing provide tailored and high-quality services for consumers [2]. Users' real-time location and the public disclosure of their mobile phone numbers could restrict the development of the IoT [3]. Because of this, it is of tremendous practical importance to investigate the Internet of Things security performance [4]. The Multimedia Vehicular Ad hoc Network (VANET) is one of the IoT-related disciplines that have received substantial interest from academia, business, and government [5]. There must be a constant flow of information from the vehicle's location and speed to the vehicle's direction and velocity to enhance traffic [6]. Smart traffic monitoring and security applications that use Wireless Multimedia Sensor Networks (WMSNs) need safe end-to-end data streaming [7].

Privacy and security must be addressed for a networked system of real-world physical things [8]. Additionally, the multimedia streams that

accompany the objects must be protected from snoopers [9]. Authentication and access control approaches can address security and privacy concerns for objects and their data under the WMSN concept [10]. Using these methods, harmful users cannot access network resources, and legal users cannot get unauthorized access to resources [11]. On the other hand, asymmetric encryption includes cypher suites requiring computationally intensive processes [12]. Existing multimedia sensors incorporated in an IoMT paradigm can not meet these demands due to their resource limitations [13]. Direct connection between sensor nodes and end-users is the most contemporary WSN/IoT method [14]. A key component of any IoT/IoMT system is the ability to communicate from machine to machine (M2M) [15].

IoT multimedia applications increasingly rely on security as a vital component [16]. The Internet of Things (IoT) is vulnerable to security threats from both applications and humans because the IoT is designed to be able to execute user-implemented applications widely [17]. It is possible to hack into applications and sensors, and hateful people can access the Internet of Things (IoT) and perform violent service assaults. A legitimate user can tamper with shared multimedia material or overly utilize network resources to interrupt services accessible to other legitimate users [18–20]. The present Internet of Things (IoT) does not have a dedicated security mechanism to deal with the threats above [21]. As a result, it is crucial and required to implement a security strategy to protect multimedia applications streaming over the IoT [22].

This paper's safety performance can be validated and contrasted with alternative approaches. For the study on the security performance of the Internet of multimedia things, it is believed that privacy protection can be implemented under the Internet of things. Four light handshake messages are transmitted to protect the transmission using Advanced Encryption Standard, and end-to-end communications can be seamlessly delivered using a revolutionary channel allocation mechanism.

The main contribution of this paper is,

- To improve vehicle safety and efficiency and fundamentally address the existing traffic congestion problem, train drivers and traffic management staff can acquire real-time information from other vehicles beyond their visual range through radios in their vehicles.
- The IoMT-WE architecture has two layers of security protection: chaotic permutation-diffusion encryption and a chaotic encryption control during sampling.

- The IoMT-WE enables multimedia sensor nodes in one cluster to access timeslots and channels from other clusters. A member node of a cluster can request a channel swap to avoid having to wait longer for a turn to send data to the head of another cluster.

Accordingly, the rest of the proposed method can be organized. Describe the relevant research in Section 2 of this paper. A summary of the planned study is provided in Section 3. Section 4 details the simulation results and discussion. Section 5 concludes the report by going into great depth on the observations and developments that have taken place.

2 Related Work

Several personal, commercial, and military applications use fibre optic networks as a common data transfer platform. Fibre optic networks have many advantages, and security remains a significant concern in their design [23]. Fibre-optic communication security was the focus of several state-of-the-art developments. Compression followed by encryption is an efficient approach to sending data efficiently and securely. This research presented the low complexity compression-based optimal homomorphic encryption (LCCE-OHE) approach for secure fibre optic transmission due to this motivation. The experimental results showed that the LCCE-OHE approach outperformed the competition in compression efficiency and had high packet loss. Real-time control and intelligent information provision for people in transportation, healthcare, smart buildings, public safety, and other fields are all possible due to these systems. Smart city programs could gather private information [24]. However, new security and privacy problems occurred when the architecture was built out. When developing the applications, these safety and privacy issues must be considered less key sensitivity.

The acceptability and widespread usage of IoT in healthcare depend on the security and privacy of patient medical data. The health data is collected from sensors and safely sent to near edge devices. In order to allow healthcare professionals easy access, devices finally send the data to the cloud [25]. Recently, the Internet of Things (IoT) and mobile health care (m-healthcare) applications have been able to offer online services in many various dimensions. For safe storage and access, many medical systems also make advantage of cloud computing technologies. So, a new Cloud and IoT based mobile health care application to provide superior services over the existing online healthcare applications [26].

Consequently, they must be taken into account while making decisions. Using the Internet of Things (IoT), smart city developers' applications could focus on the most crucial features while addressing the most pressing privacy and security issues. Information-centric smart city applications face security and privacy issues that need to be solved in the future.

Wireless communication was vulnerable to various intermediate attacks because of its unique nature. These include interference, priority violations, and spectrum poisoning. Attacks such as this pose security and privacy concerns while facilitating data transfer. By taking into account exploratory, evasion, causative, and priority violation assault, a novel approach to autoencoder deep neural network (AENN) were already devised [27]. The novel method attempted to identify the transmission results utilized to anticipate the transmission scenario, whether a jam data transfer or a sensing data transmission. Once the neural network verified that the channel was legitimate, data was sent through the network and high running time. Under the described approach, the system reduced numerous attacks on energy consumption at various stages. The appeal was due to their wide range of studies in energy efficiency, data transmission, coverage, connection, load balancing, security, dependability, scalability, and network lifespan [28]. One of the most important contributions of this research would be to present a short overview of clustering in wireless sensor networks based on three main categories such as classical, optimization, and machine learning approaches (MLA). Performance measurements and parameters were supplied for each category, and a comparative evaluation of topics such as routing protocols, dependability, and attacks in resilience was reviewed.

WSN with IoT manages all network protocols, topology, deployment of nodes, location technology, and network security. This article used the Bird Swarm Optimized Quasi-Affine Evolutionary Algorithm (BSOQAEA) to tackle the node placement problem in sensor networks [29]. Health support systems confront considerable obstacles include a lack of proper medical information, avoidable mistakes, data security risks, incorrect diagnoses, and delayed communication. Here, a wearable sensor system that is integrated with Internet of Things (IoT)-based big data mining analysis for the healthcare industry to address this problem [30]. The process was significantly sped up and high in optimization issues using a dynamic space reduction technique. Node location accuracy, minimum distance, and location error were utilized to quantify the system's efficiency. The IoMT-WE has been suggested to overcome the existing methods. The proposed method approach

has recommended improving running time, optimization issues, attacks in resilience, packet loss, and critical sensitivity.

3 Proposed Method: Internet of Multimedia Things in a Wireless Environment

IoT is implemented in agriculture through precision farming by using robots, drones, sensors, and computer imagery along with analytical tools to get insights and monitor the crops. Farms use physical equipment to monitor and collect data, which is typically used to obtain insightful information. Intelligent data gathering, waste reduction, process automation, crop diagnostics, soil improvement, and irrigation demand are benefits of adopting IoT in agriculture. Whereas, with the use of Internet of Things (IoT) technology, a smart health monitoring system that can analyze a person's temperature, blood pressure, heart rate, and levels of oxygen is being produced. There are several more applications for IoT devices in hospitals besides patient health monitoring. Patient infection can be avoided with the use of IoT-enabled hygiene monitoring equipment. IoT devices are also useful for asset managerial activities like controlling pharmacy inventories and checking refrigerator temperatures as well as controlling humidity and temperature in the environment. The memory and processing power of IoT devices are constrained, and such protocols and a common communication stack enable these devices to communicate successfully. Technical advancements in IoT operating systems (OS), data-driven intelligence in wireless networks, scheduling approaches for heterogeneous content-centric IoT, congestion avoidance tactics in IoT utilizing data science, VANETS, and IoT adoption in agricultural and healthcare IoT all benefit from these technological advances.

Figure 1 shows the Internet of Multimedia Things-based Wireless Environment. The IoMT is distinct from the IoT. More significant memory, more processing power, and a greater need for bandwidth are required. An interactive method to provide information to a user is through multimedia data. It contains a variety of data types, including textual, audio, and visual data. The major concerns with multimedia data are querying, modelling, performance, and storage. Multimedia production is more expensive than other types of production since it uses several media. Real-time deployments include industrial IoT, smart cities, smart homes, smart grids, smart agriculture, and smart hospitals. The timely and accurate transmission of data is a crucial feature of IoMT. The network must have a high quality of service (QoS) to meet these objectives. Quality of service (QoS) requirements are

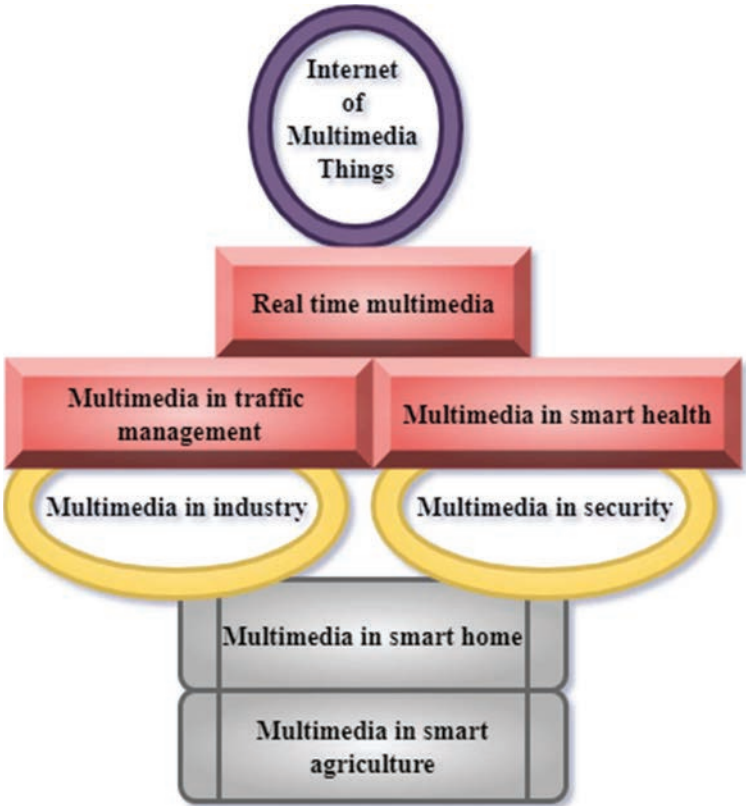

Figure 1 Internet of multimedia things based wireless environment.

technical requirements that describe the system's quality of characteristics including performance, availability, scalability, and serviceability. Business requirements that are mentioned in QoS requirements are influenced by business demands. QoS improves network performance by controlling bandwidth and giving additional resources to high-priority applications with efficient system requirements. Quality of experience (QoE) refers to the perception of QoS by the end-user (QoE). The people who utilize QoE objectively are challenging to assess as it fluctuates so much depending on the situation. Quality of Service (QoS), which represents the principle that hardware and software qualities may be assessed, improved, and perhaps guaranteed, is related to QoE but differentiates from QoS. In contrast, QoE transmits both subjective and objective user experiences. However, service providers use the network mean opinion score (NMOS) to measure the subjective quality

of experience (QoE) of their users (MOS). A Mean Opinion Score (MOS) is a metric used to quantify how well-received an activity or experience was overall according to a human reviewer. It is also referred to as the mathematical average of all individual "values on a predefined scale that a subject assigns to his assessment of the performance of a system quality". These evaluations are often acquired through a subjective quality assessment test, but they can also be predicted by an algorithm. Media data is growing at an exponential rate. Transmitting, processing, storing, and sharing data now comes with additional difficulties. Edge, fog, and cloud devices need new processing approaches. For multimedia data storage, new compression and decompression algorithms are being developed. Low-power and lossy networks, such as those found in the Internet of Things, use RPL as their standard routing protocol. Low power and lossy networks (LLNs) are a type of network in which the routers and their connectivity are both limited. LLN routers often function with restrictions on processor speed, memory, and energy (battery power). They have unstable interconnects with high loss rates and poor data speeds.

The Internet of Things (IoT) properties facilitate multimedia communication, and multimedia applications' bandwidth requirements and latency sensitivities make this communication difficult. Innovations in multimedia traffic management have been spurred by IoT's explosive rise in multimedia traffic. IoMT devices require larger memory and greater processing power to process the data they collect. Network dynamics, heterogeneity, and rigorous Quality of Service (QoS) requirements over resource-constrained IoMT offer enormous hurdles to multimedia communication. The implementation of a network-on-chip architecture can achieve improved customer satisfaction. Multimedia traffic refers to any sort of audio/visual material, whether supplied in real-time or on demand. IoT innovation is actively influencing consumer and corporate trends. The majority of the innovations made both before and during the outbreak interact with the Internet of Things either directly or indirectly. IoT advancements are generating new opportunities across a variety of industries, including healthcare, retail, automotive, and manufacturing. Multimedia in traffic monitoring, real-time multimedia, and multimedia in security are briefly explained below,

Application 1: Multimedia in Traffic Monitoring

Security applications in-vehicle networks enable users to avoid risky circumstances depending on the status of surrounding vehicles. Beacons are

security messages that are frequently and locally emitted from surrounding cars that can be collected by each vehicle. Vehicles release hazardous substances into the atmosphere, which have adverse effects on ecosystem health and human health. Transportation systems contribute to both decreasing air quality and a changing climate through emissions from burning fossil fuels. Additionally, transportation contributes to air pollution, water pollution, and ecological damage through a variety of direct and indirect interactions. There must be frequent transmission and distribution of traditional vehicle data to accomplish a high share amongst vehicles. In general, the privacy and security of the IoT and VANET are substantially compromised by this practice. The expansion of this industry is limited by the insufficiency of multimodal security performance analysis. With this research path, the multimedia VANET network is paired with IoT security research and establishing a batch authentication technique for privacy protection. Authentication is the process of identifying a device, whereas authorization provides permissions. These procedures are used by IoT devices to provide role-based access control and verify that only the access and permissions required for a task are provided.

The Internet of Things (IoT) objects collect and aggregate data elements related to their services, which represents a concern about privacy. Security and privacy are recognized as two important challenges in VANETs. To protect communication between V2V and V2I, security concerns such as confidentiality, authenticity, integrity, availability, and non-repudiation are considered.

Figure 2 shows the modelling of a multimedia VANET system. There are three types of infrastructure in the Multimedia VANET: a trusted authority (TA), roadside units (RSUs), and onboard units (OBUs). A trusted authority node has been granted permission and is in charge of maintaining an eye on the behaviour and patterns of other nodes. TA, the self-organization network registration and certification centre for fixed RSUs and OBUs, provides value-added services as the trusted management centre. There are several management domains that TA breaks down. The security channel transmits the domain-specific security parameters to the fixed RSUs. Storage, energy, and immunity to capture are common features of TAs. There are wired and wireless OBU connections to fixed RSUs. Using stationary RSUs as a bridge between OBUs and TA is secure. This information can be sent to all certified RSU groups when they have authenticated their identities with the RSUs placed in place. Data on value-added services can be sent to the automobile through TA and transferred to fixed RSUs, an intermediary.

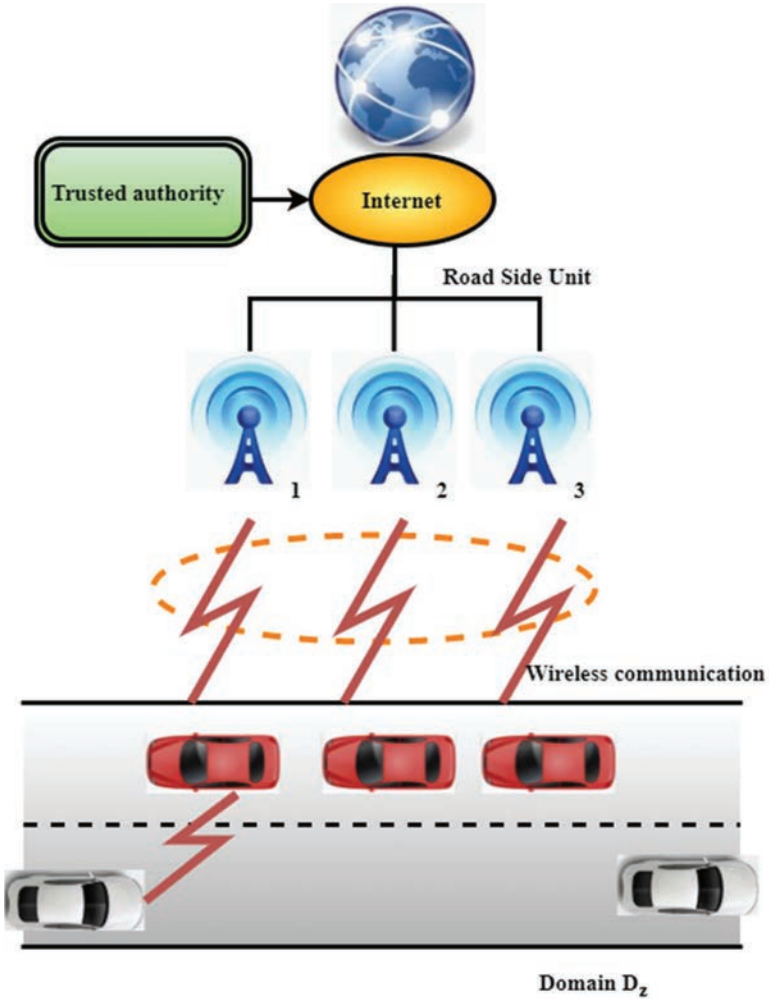

Figure 2 Modeling of a multimedia VANET system.

To secure vehicles and users, OBUs broadcast real-time traffic information to OBUs to get TA value-added services. TPDs (tamper-proof devices) are fitted in each vehicle to store and group keys and other sensitive items. For batch certification using Anonymous Batch, Data from many vehicles is sent simultaneously to fixed RSUs while a single vehicle receives traffic information from other vehicles. An aggressive attack is unavoidably impossible to defend against, regardless of the security measures in place. As a result,

this study's security performance analysis does not require sharing private data about vehicles or users.

System Initialization

The trust authority follows these steps to get the system set up.
Trust authority selects two random integers $P, P' \in H_1$ to generate the public key.
Trust authority selects one random number $r \in X_p^*$ as the private key to generate the private key.

For example, RGB-2 is used as the hash function G_j: $[0,1]^* \to X_p^*$ $(j = 0, 2, 4)$. TA chooses the hash function G_4: $H_1 \to X_p^*$ as the hash value.

RSU certificate distribution

Certificate trust authority, T_z is issued for the z_{th} TRV T_z in the domain D_z by trust authority, as follows:

The public key that is generated by randomly selecting an integer between 1 and the constant is given as $QL_{T_z} = sQ$.
Trust authority provides signatures such as the following sigma $\tau_{trust\ authority,T_z}$ including $\tau_{trust\ authority,T_z} = Sign(r, QL_{T_z} \parallel D_z)$.
The set is the private key for RLT_z. Trust authority then uses this random number to construct the public key $Cert_{trust\ authority,T_z} = QL_{T_z}, D_z, (\tau_{trust\ authority,T_z})$.

Sharing of vehicle pseudonyms and private keys

Assume that the trust authority can provide a certain number of pseudonyms to each vehicle during the annual vehicle inspection by storing them and that the time slot RT_i is split according to the length of a certain year. $R_{2,D+i-1}$ denotes the slot's length in units of the overall system. As shown in Equation (1), D time slots can be generated, each time slot's length being $[i \cdot \Delta S, (i-1) \cdot \Delta S]$. Two hash chains G_n^i can be used to produce the vehicle U_j in the pseudonym $QJE_{k,l}$ time $i's$ slot $RT_i (i \in [1, D])$ as follows:

$$\begin{cases} R_{1,i} = G_n^i(RE_{j,1}) \\ R_{2,D+i-1} = G_n^{D+i-1}(RE_{j,2}) \\ QJE_{k,l} = G_n(R_{1,i} \otimes R_{2D+i-1}) \end{cases} \tag{1}$$

$RE_{j,1}$ and $RE_{j,2}$ are the seed generation of the hash above chain, respectively.

Transmission of the Group Private Keys and the Mutual Authentication

It is possible to verify the vehicle's authenticity $\tau_{trust\ authority}$ and the road-side unit T_z using pre-stored materials and parameters. In the system model that has been deliberate and experimentally proven, there are two forms of batch verification Ver: One vehicle receives traffic data from another vehicle in a domain.

$$Ver(Q_{qvd},\ QL_{T_z} \parallel D_z, \tau_{trust\ authority,T_z}) \tag{2}$$

As shown in Equation (2), while Q_{qvd} stands for the public key of the organization that issued the certificate trust authority, the public key of the recipient, QL_{T_z}, stands for D_z's public key. After receiving D_z information, HL_i performs the following actions are stated as

$$HL_i = G(L_i^D) - L_{n+i-1}^A + f(z, y) \tag{3}$$

As shown in Equation (3), L_i^D are all variables, G is a fixed value. Group key $f(z, y)$ is calculated using the seed L_{n+i-1}^A. A batch verification Q_{qvd} of the correctness of information d is described as,

$$d\left(\sum_{l=1}^{m} g'_{k,l} Q_{qvd} - \sum_{l=1}^{m} g_{k,l} R_{k,l}, P\right) \cdot d\left(\sum_{l=1}^{m} W_{k,l} P\right) = d\left(\sum_{l=1}^{m} V_{k,l}, Q\right) \tag{4}$$

As shown in Equation (4), l is the number of values m is possible to verify a domain's information P in the cross-domain phase since $V_{k,l}$ holds the group key $g_{k,l}$. Verifying information $W_{k,l}$ from both domains is possible when R_k, obtains the group key discards after the Q cross-domain is complete. The self-healing group key D_{i-1} is changed regularly as part of this procedure as follows,

$$\begin{cases} D_{i-1} = \{s_{i-1}(z) \parallel\}\{Q_{i-1}(z)\} \\ s_{i-1}(z) = (z + QJE_{t1})(z + QJE_{t2}) \ldots (z + QJE_{tv}) \\ Q_{i-1}(z) = s_{i-1}(z) L_{n+i}^D - h(z, L_{i-1}^E) \end{cases} \tag{5}$$

As shown in Equation (5), if the domain has a revocation vehicle $s_{i-1}(z)$ or group key expiry, z can update the roadside unit's group key. The pseudonym of the revoked vehicle is represented by QJE_{t1}, $QJE_{t2}, \ldots, QJE_{tv}$. Whereas the vehicles cancelled in the $i-1$ cycle are indicated by L^{D}_{n+i} and $h(z, L^{E}_{i-1})$. Two polynomials reflect the $i-1$ period revocation and hidden polynomials $Q_{i-1}(z)$ and pj + 1(x).

Application 2: Real-time Multimedia

The term Internet of Things (IoT) refers to a network of interconnected objects capable of detecting and acting on their surroundings. They can communicate with one another through networking and the web. On the other hand, these studies do not examine the needs and constraints given by multimedia material. IoT-based architectures and protocols are being developed to facilitate multimedia content processing and transmission due to research on multimedia content, such as audio, video, and pictures. The current IoT architecture must be redesigned and turned into a new concept called the IoMT to handle real-time multimedia services and applications.

Figures 3 and 3(a) show a network's visualization and request for a channel reservation. The multimedia nodes are dispersed at random in the seamless and authorized multimedia streaming framework (SAMS). The location

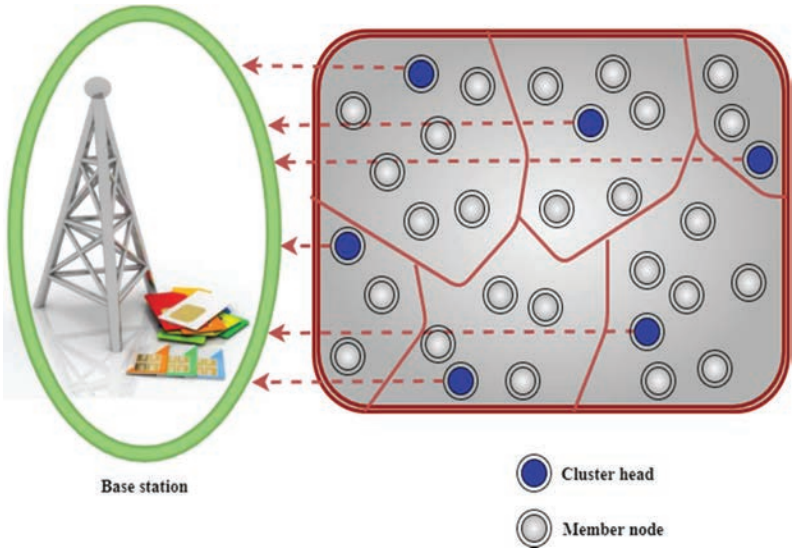

Figure 3 A network visualization.

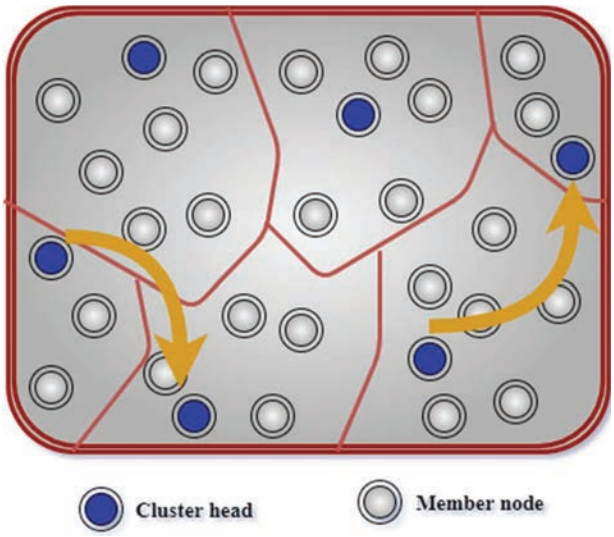

Figure 3(a) Request for a channel reservation.

of the base station is used to gather data. As previously mentioned, SAMS is composed of a setup and a steady-state phase. Two authentication stages are implemented during the setup process to keep the network safe from intruders. As each node successfully authenticates, the clusters are formed, and each node is assigned to one of the cluster heads as its primary point of contact. The steady-state phase focuses on the continuous transmission of information inside the cluster and across surrounding clusters. In the star topology, a hub is used to link every computer. All other nodes are connected using one cable, which is referred to as the central node. It is most often used on LAN networks since they are cheaper and simple to set up. The central nodes take data from their local sub-network and send it to other central nodes on a different carrier frequency while being powered by the structure's electrical grid. Nodes on separate segments cannot communicate with one another directly, but by building a bridge across the segments, communication between the nodes is made possible. When a packet is designed for a host on the opposite side, the bridge allows it to transmit the information. The cluster's central node receives multimedia data from all of the nodes. The member nodes can record images and video files. A video is a collection of unique frames processed consecutively. There are 10 video frames in a GoP, and a sequence of samples is used to process the Group of Pictures (GoP). The buffer threshold for each node is achieved after six GoPs.

The data is dropped, or a channel reservation request is sent to the nearest cluster head, depending on the behaviour of the nodes in the cluster. A member node can broadcast data to the base station through its own or a nearby cluster head, and a channel allocation request is started by a member node in the latter scenario. Wireless Multimedia Sensor Networks (WMSN) are implemented in severe conditions and are vulnerable to numerous threats and assaults compared to conventional networks. The development of Wireless Multimedia Sensor Networks (WMSNs) has changed the focus from conventional scalar wireless sensor networks to networks containing multimedia devices that can retrieve scalar sensor data as well as video, audio, and image data. Due to the accessibility of low-cost CMOS cameras and microphones, as well as the substantial advancements in distributed signal processing and multimedia source coding techniques, WMSNs can deliver multimedia material. These networks do not support complex and resource-intensive security mechanisms because of their limited energy supply. Our investigation into the attack models in WSNs/WMSNs and the different harmful behaviours that endanger SAMS's operating mechanism helps us assess the security of this network management system. Retransmission of previously sent packets by an adversary reduces the freshness of data and wastes network resources. Disk operating Systems (DoS) D_s aim to prevent valid nodes from accessing network resources by interrupting the services offered by a specific cluster head. Flooding the cluster heads with too many requests is a common way to cause DoS. As Sybil S_m Explains that an attacker uses several identities to gain unauthorized access to network resources. Eavesdropping E_{dr} an attacker steals data in transit from legitimate nodes to eavesdrop on the real-time conversation.

Channel reservation

Node E_{dbq} within a cluster continually detects the environment and saves any collected data DG_k in its buffer, which is constrained by a predetermined threshold given as,

$$\sum E_{dbq} \rightarrow \begin{cases} DG_k, & if\ m_n > m_r, \\ DG_{MA} & otherwise \end{cases} \tag{6}$$

As shown in Equation (6), a broadcasts DG_{MA} to its m_n while communicating inside the cluster. The capture rate m_r is more significant than its transmission rate in this situation. During the first stages of network deployment DEk and cluster formation $\frac{d}{dr}E_{dbq}$. The buffer of each i is empty

since they have not yet sensed their surroundings m_{ki} are described as

$$\sum_{k=1}^{DE_{dbq}} \sum_{i=1}^{z} DEk \frac{d}{dr} E_{dbq}(m_{ki}) = \sum_{i=1}^{z} \frac{d}{dr} E_{tra}(m_i z) \tag{7}$$

As shown in Equation (7), the maximum number of member nodes $E_{tra}(m_i z)$ associated with a specific cluster head z and the total number of cluster heads that are represented by DE_{dbq} and k, respectively. To prevent the packet loss of DE_{dbq} a member node i must act promptly. Each member node must use a channel accessible with $E_{dbq}(m_{ki})$ instead of waiting for its allotted $E_{tra}(m_{ik})$ to be assigned as follows,

$$\sum_{k=1}^{DE_{dbq}-1} \sum_{i=1}^{z} DE_{MA} \frac{d}{dr} E_{dbq}(m_{ki}) = \sum_{k=1}^{b} \frac{d}{dr} E_{tra}(m_{ik}) \tag{8}$$

As shown in Equation (8), a cluster head k for all member nodes in that specific cluster b; hence it's vital to specify z accordingly. The same cluster head, on the other hand, serves as a DE_{MA} for the nodes that constitute an additional cluster.

Algorithm 1: WMSN's Multimedia Streaming

Initialization:

Nodes in a cluster are given slots T_s by their cluster heads.

To collect data, each node in the network has a sense of its surroundings E_{dbq}.

Each node in the cluster keeps tabs on how much of its buffer is currently occupied m_n.

Input: $\{m_n, m_r, E_{dbq}, T_s\}$

j detects the environment.

if ($m_n < m_r$)+ T_s is true then

$j \rightarrow DEk$: $\{E_{dbq}$ Communication inside a cluster is initiated$\}$

else

$j \rightarrow DG_{MA}$

j sets a response timer of T_r.

DG_{MA} searches for any accessible T_s

if true then

$DG_{MA} \rightarrow j : \{D_{gn}\}$.

else

j is waiting for its turn T_s.

end if

if $MD_{gn} < T_r$ then

$j \rightarrow DG_{MA}$: $\{E_{dbq}$, communication outside a cluster is initiated$\}$.

else

j verifies the availability of its resources T_s

if true then

$j \rightarrow DEk$: $\{E_{dbq}\}$

end if

end if

end if

Algorithm 1 shows the WMSN's multimedia streaming. A subset of the IoT, Wireless sensor networks (WSNs) serves as a data collection tool for j numerous applications connected to the Internet of Things. Its heterogeneity and power consumption requirements necessitate several protocols being developed to enable the WSN in multimodal IoT. Member nodes that T_r requests channel allocation DG_{MA} to are counted. Finally, we computed solely for those network members that send their E_{dbq} to their DEk.

Application 3: Multimedia in Security

An improvement over IoT in terms of interactivity and cooperation across heterogeneous multimedia objects is possible with the Internet of Multimedia Things (IoMT). Sensors that collect multimodal data, such as IoMT and big data, are becoming more commonplace. There are two key challenges to overcome in gathering these large amounts of multimedia data. Sensors cause limited computer resources and huge data quantities. To save on transmission bandwidth and sensor power, it's worth mentioning that compression encoding is an option. Another issue is ensuring the security of the data throughout and after the sampling process. Even if the sensors have been hacked, no one can get their hands on critical information. Figure 4 illustrates the compressive sensing (CS) data-gathering method based on

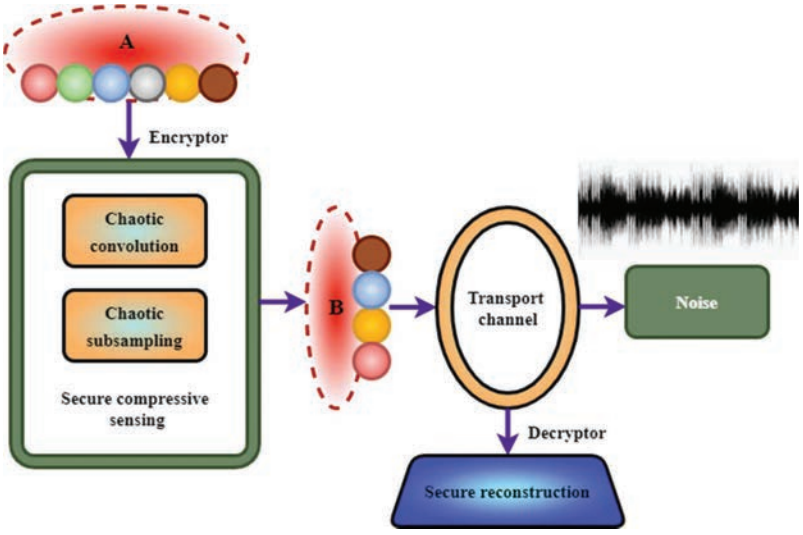

Figure 4 CS data gathering method based on CCS.

chaotic convolution and subsampling (CCS). Compressive sensing (CS) is a mathematically elegant method for decreasing the sampling rate, which may enable context awareness on a wider variety of devices. However, practical problems with the sampling and reconstruction methods, particularly for heterogeneous ubiquitous devices, limit the spread of CS in real-world environments. The chaotic systems used in the CS measurement matrix are intended to make it deterministic. While maintaining the majority of the characteristics of the random CS matrix, this chaotic compressed sensing (CCS) measurement matrix is easier to implement in hardware.

When it comes to gathering IoT data, CS has emerged as a promising technology that can meet the standards set out by the first challenge. If the sampled information is sparse, sampling and compression can be performed concurrently. When using CS, a large portion of the computational complexity is moved from sampling to reconstruction since sampling is linear in data dimension, and rebuilding is cubic. This is what the Internet of Things (IoT) is looking for in terms of CS's positive properties. According to this insight, CS technology has been advocated for IoT applications in several papers. Noise in the real transport channel typically obscures the encrypted image, necessitating a high-quality encryption technique to avoid being harmed. An image's quality is assessed using Gaussian noise and Salt and Pepper noise in a noisy environment.

Encryption process

Step 1: Process image signals using chaotic convolution and subsampling, starting with the first image signal and working backwards. An image signal z_j is represented by y_j of size $(M/m) \times 1$ that indicates the measuring outcome $j = 1, 2, \ldots m$.

$$z_j = \psi y_j$$

Step 2: The sampled pictures z_j are shared into a single master image Z.

Step 3: Use transform to Z and record the modified output as Z_1.

Step 4: Single-value diffusion can be used to disperse Z_1 and identify the outcome as Z_2.

Decryption process

The decryption design has the following steps.

Step 1: Z_2 has to be subjected to the inverse single-value diffusion. XOR's inverse can be easily computed, and the decrypted output is Z_1.

Step 2: Transform to Z_1 can be used. Decryption produces Z.

Step 3: Separate Z into m images z_j, $j = 1, 2, \ldots m$.

Step 4: The total variation optimization approach can be used to reconstruct m images z_j.

Figure 5 shows the optical depiction of the fundamental framework. The developed system allows for batch image processing, which samples, compresses, fuses, and encrypts multiple images at once. The service flow of the design can be summarised as follows. In a sensor node, numerous picture signals are initially convoluted one at a time by chaotic convolution before being subsampled by chaotic systems. Secure CS is used in chaotic convolution and subsampling to accomplish sampling, compression, and encryption, which is a solution to the first challenge issue. As firmly developed, the CS-based method is insufficiently secure. Using the help of fusion encryption, users can combine numerous subsampled images into a single master image, which one can then further encrypt with widely used image encryption techniques.

Simple cascading combines the master images, and Zig-zag scanning techniques can be employed depending on the situation's specific needs. For image encryption, permutation and diffusion processes are described

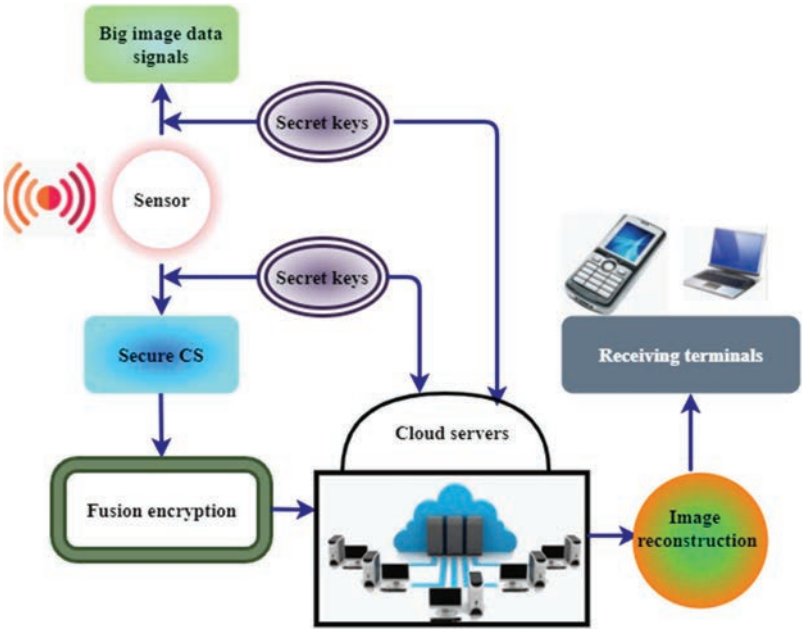

Figure 5 Optical depiction of the fundamental framework.

using the Arnold transform and single-value diffusion. For an ideal picture cipher, this encryption has the qualities of confusion and dispersion. It is uploaded to cloud servers with enormous storage and computing capacity to store, decode, and rebuild the finished encrypted picture.

Compressive sensing (CS)

Signal sampling and reconstruction theory state that sample rates must be at least twice as fast as the bandwidth of a signal to ensure proper reconstruction. Low-dimensional structures or those with relevance and cyclical properties can be used to explain the vast majority of data. As a consequence, when sampling Nyquist samples, some redundancy is prevalent. According to the CS theory, the convergence of the Nyquist theory is not necessary for a high-probability reconstruction of the compressible signal. Utilize an orthogonal transform matrix χ_{ik} to describe the sparseness of a one-dimensional signal M as follows,

$$y = \sum_{i=1}^{M} r_i \chi_{ik} = \chi r \tag{9}$$

As shown in Equation (9), i denotes the majority of the components are zeros in a y vector and is said to be r_i sparse if it includes just χr nonzero values. To get a linear measurement of the original signal ψ, the construction of an irrelevant matrix to the transformation matrices. The optimization issues z is defined as,

$$z = \psi y = \psi \chi r = \odot r \tag{10}$$

As shown in Equation (10), where y is chosen by the random matrix's unique limitations χr. The sensing matrix for reconstruction is denoted by $\odot r$. The random convolution d_{j-1} is controlled by a chaotic system $u_1 u_2$ if it is termed chaotic convolution as follows,

$$d_{j-1} = \begin{cases} u_1 u_2 d_j (1 + u_2 d_j), & d_j > 1.5 \\ u_1 u_2 (1 + d_j)(1 + u_2 (1 - d_j)), & d_j \leq 1.5 \end{cases} \tag{11}$$

As shown in Equation (11), using a chaotic system to randomly choose certain indices in an image signal, chaotic subsampling d_j is a technique for sampling images. An image's pixels Y_{l-1} can be jumbled up using the Arnold transform M. By repeatedly transforming an image Z_{l-1}, the connection c between its pixels can be eliminated Z_l is defined as,

$$\begin{bmatrix} Y_{l-1} \\ Z_{l-1} \end{bmatrix} = mod \left(\begin{bmatrix} 1 & d \\ c & cd - 1 \end{bmatrix} \begin{bmatrix} Y_l \\ Z_l \end{bmatrix}, M \right) \tag{12}$$

As shown in Equation (12), an image can be returned to its original state d using Arnold transforms if they are applied to a Y_l restricted number of changes. The single value diffusion shows that a secret key sensitivity of each pixel value is independently expressed as,

$$\psi' + \psi = (\psi \oplus d) + (\psi' \oplus d) \tag{13}$$

As shown in Equation (13), the plaintext is represented by ψ' and the ciphertext by ψ. Iterating cascading chaotic systems with initial key d supplies the secret key in this case. It is possible to conceive of random convolution as a sampling method in which a random pulse is added to the original signal zx is given as,

$$zx = 1/\sqrt{M} \cdot E^* \Theta E z \tag{14}$$

As shown in Equation (14), where E is the discrete Fourier (DF) matrices, E^* is the inverse (DF) matrices, and Θ is the diagonal matrices.

Setup Phase

When a multimedia node k enters the system, running time in the base station (BS) F_k provides it with a 16-bit number that is used for authentication at various levels F_{avg} are stated as,

$$F_{avg} + sur_{JC} = \sum_{k=1}^{M} \frac{F_k}{M} + N[\upsilon_{dgk} \oplus JC_{DF_k} \oplus JC_{AR}] \tag{15}$$

As shown in Equation (15), sur_{JC} encryption and decryption prevent one or more attackers M from being able to choose a cluster head N. Furthermore, this approach assures that only those nodes υ_{dgk} identified by JC_{DF_k} can operate as JC_{AR}. The least expensive Exclusive cryptographic procedure σ_k in terms of resources JC_{DF_k} and compute as follows,

$$IDe_j = N[JC_k, JC_{DF_k}, \sigma_k] \tag{16}$$

As exposed in Equation (16), join demand control packet IDe_j is created by each k and sent to a JC_k. Received Signal Strength Indicator (RSSI) values N that are among the highest possible. To construct a 256-bit encrypted challenge, an operation is conducted on N and δ_{chlg}, resulting in a 128-bit cypher that is added to μ_k is given as

$$\delta_{chlg} = N[\{\mu_k, (\mu_k \oplus R_l \backslash \upsilon_{DG_k})\} AES256] \tag{17}$$

As shown in Equation (17), υ_{DG_k} is the one-time usage of a pseudorandom identifier throughout the whole cryptographic transaction R_l. In Cipher Block Chaining (CBC) mode, users employed an Advanced Encryption Standard AES with a key length of 128 bits to produce a challenge. The proposed method improves running time, optimization issues, attacks in resilience, packet loss, and key sensitivity.

4 Result and Discussion

To ensure more unpredictability and statistical convergence, users conducted trials with varying node densities and BS locations. A scalar integer's buffer size is the maximum size of consecutive data from each network interface that a node can store. Therefore, [31] 10 data has been taken to compare IoMT-WE to the existing methods of different performance parameters, such as running time, optimization issues, attacks in resilience, packet loss, and key sensitivity.

Table 1 Running time analysis

Image	Encryption Time(s)	Decryption Time(s)
Tom	2.552774	556.742421
Photographer	2.552774	487.271348

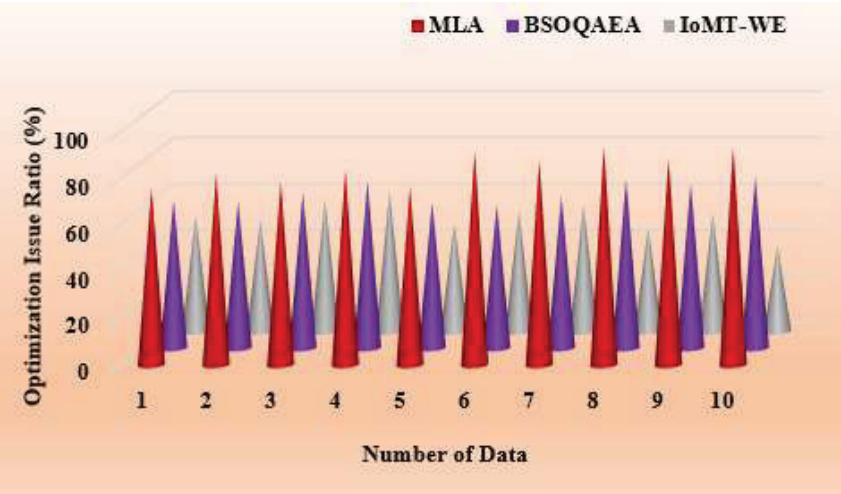

Figure 6 Optimization issue.

Table 1 shows the running time it takes to encrypt and decrypt data and the time it takes to decode data. Because the suggested encryption scheme is both fast and secure, it can be used to acquire data while protecting its privacy quickly. Using mathematical units of computation, asymptotic analysis calculates the running time of every process. As derived in Equation (15), the general block operation mode, the suggested encryption architecture, offers parallel processing, which can further decrease encryption time. Decryption takes a long time, and however, it can be fixed rapidly on cloud servers with a lot of computing power. Compared to the existing method, the proposed method improves the running time.

Figure 6 shows the optimization issue. According to the suggested framework, they find the shortest path between nodes in the optimization issue. Communication capability and range vary across the nodes. As derived in Equation (10), the cost of the bidirectional connection is calculated to determine the route. The shortest route problem has been broadened to include this issue. This study proposes a novel optimal approach that considers the intercluster level and the local level of clusters. Compared to the existing method,

Table 2 Attacks in resilience

Attacks	Existing Method	Proposed Method
$\boldsymbol{D_s}$	Yes	Yes
$\boldsymbol{S_m}$	Yes	Yes
$\boldsymbol{E_{dr}}$	No	Yes
$\boldsymbol{I_{rj}}$	Yes	Yes
$\boldsymbol{R_p}$	No	Yes

the proposed method reduces the optimization issue by (36.8%). Cluster Heads (CHs) decide the local routing pathways based on the distance of nodes from one other. At the same time, the transmission algorithm determines the inter-cluster routing paths through the use of cluster coordinators (CCOs). A static routing approach reduces the path's complexity.

Table 2 and Equation (18) show the attacks in resilience. The two-level authentication's sturdiness is tested against the strength of the competition's solutions. Pseudorandom number $\boldsymbol{R_p}$ is used to create DEk, which is then added to a timer T_k. Attackers can have a tough time replaying packets with this combination of T_k and $\boldsymbol{R_p}$. These tactics are more vulnerable to passive replay $\boldsymbol{R_p}$ assaults than the others.

$$DEk = 1 \times R_p + \frac{1}{(T_k + D_{\boldsymbol{s}})} \sum_{\boldsymbol{j=1}}^{\boldsymbol{J}} I_{rj} \tag{18}$$

Each time a new round is completed in the system, a new set of cluster leaders is chosen. This decision prevents an attacker from conducting DoS $\boldsymbol{D_s}$ attacks. Insiders cannot participate in the authentication process because of J and j. Security primitives cannot be distributed before authentication in this technique, which makes them vulnerable to hostile insider $\boldsymbol{I_{rj}}$ attacks.

Figure 7 shows the packet loss. As derived in Equation (8), IoMT-WE intra-cluster communication involves each k waiting its turn to broadcast E_{dbq} using its assigned m_{ki}. DE_{MA} assigns spare channels for inter-cluster communication, which reduces the average packet loss. Nodes in the IoMT-WE cluster communicate with each other through DEk and DE_{MA} respectively, for inter/intra-cluster communication. Compared to intra-cluster communication, the packet loss for the proposed system is much reduced. This is primarily due to the DE_{MA} position in the sensor field and the underlying channel allocation mechanism. Compared to the existing method, the proposed method reduces packet loss by (42.5%).

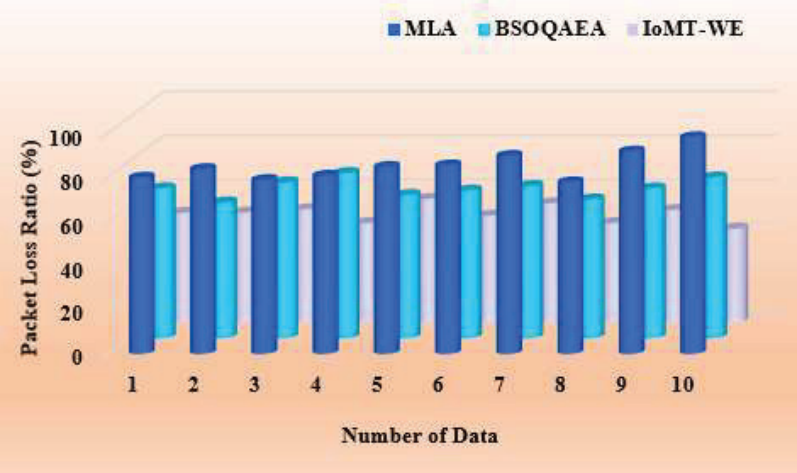

Figure 7 Packet loss.

Table 3 Key sensitivity

Image	Analysis of Correct Key	Analysis of Wrong Key	Analysis of Correct Key
Tom	6.8676	12543	12845
Photographer	9.4738	21748	21952

Table 3 shows the key sensitivity. The general chaotic system's high sensitivity to the system's starting parameters and values suggests that the algorithm's proposed key sensitivity is high. The decoded Tom and Photographer images with the right keys provide visual proof. With a disturbance level, the instances of keys are just slightly shaken. It is possible to see even a slight variation leads to a decoded signal that is nearly unrecognizably altered, as seen in Equation (13). Mean square error (MSE) is a method for determining the key's sensitivity in digital verification. The original image does not provide valuable information even if the erroneous key has a minor departure from the right one. Therefore, the suggested architecture is very sensitive to the keys. The proposed method evaluated running time, optimization issues, attacks in resilience, packet loss, and key sensitivity.

5 Conclusion

The IoMT-WE aims to address the issues of vehicle information sharing and user privacy. The broadcast revocation list's communication cost and privacy problems can be avoided by using conditional privacy and batch validation in

this method. The recommended design features a security technique based on chaotic encryption. In other words, the sampling approach should contain a CCS process. The suggested strategy can effectively safeguard data collecting at a minimal computational cost. Batch processing of large image data sets is possible within the suggested framework. During the steady-state phase, the development of these clusters allows for the steady and dependable transfer of traffic from member nodes. There is a predefined threshold for the size of each node's buffer. When a node in a cluster reaches this threshold, it borrows a spare channel from the cluster head of a nearby cluster. In the future, researchers want to investigate the effect of multimedia nodes' on the wireless environment and data collecting and transmission to minimize communication overhead. The experimental outcome suggested that the proposed method improves running time, optimization issues, attacks in resilience, packet loss and key sensitivity.

References

[1] Obeidat, H., Shuaieb, W., Obeidat, O., and Abd-Alhameed, R. (2021). A review of indoor localization techniques and wireless technologies. *Wireless Personal Communications*, *119*(1), 289–327.

[2] Safaldin, M., Otair, M., and Abualigah, L. (2021). Improved binary gray wolf optimizer and SVM for intrusion detection system in wireless sensor networks. *Journal of ambient intelligence and humanized computing*, *12*(2), 1559–1576.

[3] Manikandan, S., and Chinnadurai, M. (2021). Effective energy adaptive and consumption in wireless sensor network using distributed source coding and sampling techniques. *Wireless Personal Communications*, *118*(2), 1393–1404.

[4] Almutairi, A. F., Al-Gharabally, M., and Salman, A. A. (2021). Particle swarm optimization application for multiple attribute decision-making in vertical handover in heterogeneous wireless networks. *Journal of Engineering Research*, *9*(1).

[5] Chaves, P. R., Assumpção, R. M., Ferreira, L. C., Cardieri, P., Branquinho, O. C., and Fruett, F. (2021). A remote emulation environment for the teaching of low-power wireless communications. *Computer Applications in Engineering Education*, *29*(6), 1453–1464.

[6] Singer, A., and Robinson, J. T. (2021). Wireless power delivery techniques for miniature implantable bioelectronics. *Advanced Healthcare Materials*, *10*(17), 2100664.

[7] Dekkers, G., Rosas, F., van Waterschoot, T., Vanrumste, B., and Karsmakers, P. (2022). Dynamic sensor activation and decision-level fusion in wireless acoustic sensor networks for classification of domestic activities. *Information Fusion*, *77*, 196–210.

[8] Furqan, H. M., Solaija, M. S. J., Türkmen, H., and Arslan, H. (2021). Wireless communication, sensing, and REM: a security perspective. *IEEE Open Journal of the Communications Society*, *2*, 287–321.

[9] Singh, P., and Mittal, N. (2021). An efficient localization approach to locate sensor nodes in 3D wireless sensor networks using adaptive flower pollination algorithm. *Wireless Networks*, *27*(3), 1999–2014.

[10] Bashar, A., and Smys, S. (2021). Physical Layer Protection Against Sensor Eavesdropper Channels in Wireless Sensor Networks. *IRO Journal on Sustainable Wireless Systems*, *3*(2), 59–67.

[11] Rawat, P., and Chauhan, S. (2021). Clustering protocols in wireless sensor network: A survey, classification, issues, and future directions. *Computer Science Review*, *40*, 100396.

[12] Rezaeipanah, A., Amiri, P., Nazari, H., Mojarad, M., and Parvin, H. (2021). An energy-aware hybrid approach for wireless sensor networks using re-clustering-based multi-hop routing. *Wireless Personal Communications*, *120*(4), 3293–3314.

[13] Rodríguez, D. Z., Carrillo, D., Ramírez, M. A., Nardelli, P. H., and Möller, S. (2021). Incorporating wireless communication parameters into the E-model algorithm. *IEEE/ACM Transactions on Audio, Speech, and Language Processing*, *29*, 956–968.

[14] Abdulsahib, G. M., and Khalaf, O. I. (2021). Accurate and effective data collection with minimum energy path selection in wireless sensor networks using mobile sinks. *Journal of Information Technology Management*, *13*(2), 139–153.

[15] Kanoun, O., Bradai, S., Khriji, S., Bouattour, G., El Houssaini, D., Ben Ammar, M., … and Viehweger, C. (2021). Energy-aware system design for autonomous wireless sensor nodes: A comprehensive review. *Sensors*, *21*(2), 548.

[16] Ostovar, A., Keshavarz, H., and Quan, Z. (2021). Cognitive radio networks for green wireless communications: an overview. *Telecommunication Systems*, *76*(1), 129–138.

[17] Dey, P., Kumar, C., Mitra, M., Mishra, R., Chaulya, S. K., Prasad, G. M., … and Banerjee, G. (2021). Deep convolutional neural network-based secure wireless voice communication for underground mines.

Journal of Ambient Intelligence and Humanized Computing, *12*(10), 9591–9610.

[18] K. Rajakumari, P. Punitha, R.L. Kumar and C. Suresh, Improvising packet delivery and reducing delay ratio in Mobile ad hoc network using neighbor coverage-based topology control algorithm, International Journal of Communication Systems, 35 (2), 2022.

[19] Manogaran, G., Varatharajan, R., Lopez, D., Kumar, P.M., Sundarasekar, R. and Thota, C., 2018. A new architecture of Internet of Things and big data ecosystem for secured smart healthcare monitoring and alerting system. Future Generation Computer Systems, 82, pp. 375–387.

[20] Nayak, P., Swetha, G. K., Gupta, S., and Madhavi, K. (2021). Routing in wireless sensor networks using machine learning techniques: Challenges and opportunities. *Measurement*, *178*, 108974.

[21] Almalki, F. A. (2021). Developing an adaptive channel modelling using a genetic algorithm technique to enhance aerial vehicle-to-everything wireless communications. *Int J Comput Networks Commun*, *13*(2), 37–56.

[22] Khashan, O. A., Ahmad, R., and Khafajah, N. M. (2021). An automated lightweight encryption scheme for secure and energy-efficient communication in wireless sensor networks. *Ad Hoc Networks*, *115*, 102448.

[23] Venu, D., Mayuri, A. V. R., Neelakandan, S., Murthy, G. L. N., Arulkumar, N., and Shelke, N. (2022). An efficient low complexity compression-based optimal homomorphic encryption for secure fibre optic communication. *Optik*, *252*, 168545.

[24] Al-Turjman, F., Zahmatkesh, H., and Shahroze, R. (2022). An overview of security and privacy in smart cities' IoT communications. *Transactions on Emerging Telecommunications Technologies*, *33*(3), e3677.

[25] Thota, C., Sundarasekar, R., Manogaran, G., Varatharajan, R. and Priyan, M.K., 2018. Centralized fog computing security platform for IoT and cloud in healthcare system. In Fog computing: Breakthroughs in research and practice (pp. 365–378). IGI global.

[26] Kumar, P.M., Lokesh, S., Varatharajan, R., Babu, G.C. and Parthasarathy, P., 2018. Cloud and IoT based disease prediction and diagnosis system for healthcare using Fuzzy neural classifier. Future Generation Computer Systems, 86, pp. 527–534.

[27] Ali, S. M., Elameer, A. S., and Jaber, M. M. (2022). IoT network security using autoencoder deep neural network and channel access algorithm. *Journal of Intelligent Systems*, *31*(1), 95–103.

[28] Amutha, J., Sharma, S., and Sharma, S. K. (2021). Strategies based on various aspects of clustering in wireless sensor networks using classical, optimization and machine learning techniques: Review, taxonomy, research findings, challenges and future directions. *Computer Science Review*, *40*, 100376.

[29] Malathy, E. M., Asaithambi, M., Dheeraj, A., and Arputharaj, K. (2022). Hybrid bird swarm optimized quasi affine algorithm based node location in wireless sensor networks. *Wireless Personal Communications*, *122*(2), 947–962.

[30] Muthu, B., Sivaparthipan, C.B., Manogaran, G., Sundarasekar, R., Kadry, S., Shanthini, A. and Dasel, A., 2020. IOT based wearable sensor for diseases prediction and symptom analysis in healthcare sector. Peer-to-peer networking and applications, 13(6), pp. 2123–2134.

[31] https://www.kdnuggets.com/2017/01/machine-learning-cyber-security.html

Biographies

Nabeel Mahdy Haddad is a lecturer at Misan University, Iraq. He completed his PhD at the University of Southern Queensland, Australia, his interest is Machine Learning.

Mustafa sabah Mustafa is a lecturer at Dijlah University College, His interest area is Deep Learning.

Hayder Sabah Salih received his B.Sc Degree in computer engineering from Baghdad university Iraq, Baghdad in 2007, an M.Sc Degree in computer engineering from Moscow Automotive and road construction state technical university (MADI) in 2013, and a Ph.D. Degree in computer engineering/information technology and systems from Tambov State Technical University in 2020, currently he is holding the position of the head of the Scientific Affairs section in the Department of Private Education in Mohesr, Iraq.

Mustafa Musa Jaber is a PhD holder from the technical university of Malaysia and he received a postdoctoral from University Tun hussein Onn Malaysia, his interest in telemedicine, machine learning, and the human factor. Currently working as head of the department of information technology, Dijlah University College, Baghdad, Iraq.

Mohammed Hasan Ali is a Senior Researcher in the Artificial Intelligence & Machine Learning Lab Imam Ja'afar Al-sadiq University. He received his PhD from Faculty of Computing System and Software Engineering Universiti Pahang Malaysia in 2016 and 2019 respectively. Currently working as head of Research Center, Imam Ja'afar Al-sadiq University, Iraq.