Centralized Infrastructure-Aware Reliable Data Transaction Model in IoT-Enabled MANET and Cloud Using GWO and Attention Mechanism with LSTM

Dinesh Kumar Reddy Basani[1,*], Sri Harsha Grandhi[2], Qamar Abbas[3]

[*1]CGI, British Columbia, Canada. Email: dineshkumarreddybasan@ieee.org
[2]Intel, Folsom, California, USA. Email: sriharshagrandhi@ieee.org
[3]Faculty of Computing and Information Technology, International Islamic University, Islamabad, 44000, Pakistan.
Email: qamar.abbas@iiu.edu.pk

ABSTRACT

Despite the advantages of using IoT-enabled Mobile Ad hoc Networks (MANETs) in smart cities, healthcare, and military operations, transmission needs to be efficient and secure. This investigation introduces a "Centralized Infrastructure-Aware Reliable Data Transaction Model" which calibrates network speed and security in these scenarios. For secure data transmission and low computation cost, Edward prime curve cryptography (EPCC) is used and selects the most efficient cluster heads for managing data routing using Grey Wolf optimization (GWO). It also includes a reactive routing algorithm like Ad hoc On-demand Distance Vector (AODV) routing which provides the high reliability of data sent and received dynamically by an effective path discover method. It achieves more success rate, efficiency, and privacy than the others, including K-Nearest Neighbor (KNN), Collaborative Computing Trust model CCTM, and Quality of Service QoS in data transfer. The figures show that every element is important (the ablation study achieved a 93% success rate and got the entire model to an accuracy of 92.5%) in this example situation — but it still explains why embeddings are biased by definition. This hybrid approach is ideal for capacity-heavy applications across numerous industries, as it provides a reliable and secure network solution.

Keywords: MANETs, IoT, EPCC (Edward Prime Curve Cryptography), GWO, AODV, Data Security.

1. INTRODUCTION

With the advent of IoT, and hence using MANETs for smart cities, healthcare applications, military operations, etc., there is an increasing need to transmit data safely and reliably over such networks. Although MANETs are famous for their dynamic architecture and adaptable nature, they often become susceptible to security attacks along with inefficient routing of data due to the presence of a decentralized approach in such networks. To address these issues, this dissertation proposes a "Centralized Infrastructure-Aware Reliable Data Transaction Model" which can be utilized for cloud computing and Internet of Things-enabled MANETs. This is implemented by combining the Grey Wolf Optimization (GWO) method with an Attention-based Long Short-Term Memory (LSTM) model to enhance both security and efficiency. GWO minimizes the end-to-end latency of ADL in MANET by selecting optimum cluster heads which enhances network performance and reduces routing delays. Meanwhile, the LSTM attention mechanism helps in enhancing the system's capability to pay more attention to vital data attributes. The hybrid approach operates better for dependable and safe data delivery in vibrant also attackprone environments.

Corresponding Author Name: Dinesh Kumar Reddy Basani,
Corresponding Author mail: dineshkumarreddybasan@ieee.org

Wireless device-to-device communication gained popularity in decentralized environments and frequently ran over the so-called Mobile Ad Hoc Networks, MANETs. In this network, data routing should be carried out by a mobile node instead of a centralized infrastructure.
The Mobile Ad hoc Networks (MANETs) plays a significant role in the historical context. This method was

very flexible, it had inconsistencies in data routing as well as a few security issues since the nodes could talk to each other. ECC (Elliptic Curve Cryptography) and blockchain technologies have been incorporated into MANETs as a security output to protect data. In addition to this, machine learning models such as Support Vector Machines and Random Forest are used for intrusion detection. Unfortunately, these methods often fail to provide reliable data transmission and optimal routing efficiency. This work is an extension of previous research in terms of combining a centralized infrastructure along with the latest optimization and prediction algorithms for better performance of MANET.

In this model, we introduced some key technical innovations to improve the security and reliability of data transmission in MANETs with Internet of Things features. To select the optimal cluster heads, and reduce routing decision time to enhance network performance Grey Wolf Optimization (GWO). GWO can also balance the exploration (versus exploitation) based on other methods, and that is why GWO is more effective than some of the previous algorithms mentioned above which can stuck in local optima. Intrusion detection will be improved, and information on potential threats can just be obtained by using LSTM networks in an attention mechanism that only focuses on the important parts of time-series data. To further enhance public safety top of mind with this model, also incorporates state-of-the-art cryptographic protections that are in place to protect their most sensitive information, such as Edward Prime Curve Cryptography (EPCC). By including centralized monitoring, the system can quickly detect rogue nodes or rejoin attempts, making it suitable for practical use.

1.1 Objectives

- Presenting an integrated system for ensuring reliable and secure data transfer into cloud, IoTdriven MANETs.
- Grey Wolf Optimization (GWO) can select cluster heads to ensure the maximum possible energy savings and best network performance
- Detect security risks more accurately by combining Long Short-Term Memory (LSTM) with an attention technique.
- Use cutting-edge encryption methods, including Edward Prime Curve Cryptography (EPCC), to protect consumer data.
- Use trust-based fuzzy systems to assess and validate data transmission paths to guarantee reliable and secure communication connections.

This study proposes a novel "Centralized Infrastructure-Aware Reliable Data Transaction Model" that combines Grey Wolf Optimization (GWO) for optimal cluster head selection and an attention-based Long Short-Term Memory (LSTM) network to enhance data security and efficiency in IoT-enabled MANETs. The key contributions include improved performance in data reliability, privacy, and success rates compared to existing models such as KNN and CCTM, along with the innovative use of Edward Prime Curve Cryptography (EPCC) for secure data encryption. The remainder of the paper is structured as follows: a review of related literature and contextual background is presented in Section 2; the methodology, emphasizing GWO and LSTM integration, is detailed in Section 3; experimental results and discussions are provided in Section 4; and the study concludes with key insights and future directions in Section 5.

2. LITERATURE SURVEY

[1] present a framework for the efficient scheduling of different workload types in data centers, to decrease energy costs Instead, they take into account job features such as whether additional memory or processing capacity is needed and the power and cooling systems of a data center. The recommended scheduling policy reduces the peak power consumption and its corresponding operational cost by adapting runtime resource allocation according to current conditions. This investigation results find an increased use of resources, and energy-saving when using the infrastructure-aware scheduling technique than in common scheduling techniques.

[2] highlight the imperative necessity of a new paradigm in urban water infrastructure to be based on both sustainability and resilience. They emphasize decentralized systems, drivers of decentralization, and scaling appropriate for decentralization, which offers an optimal balance between costs, governance, resilience, and recycling that support sustainable UWI planning, both in developed and developing countries.

[3] review centralized versus decentralized cloud computing architectures over healthcare, focusing on such architectures' impact on systems of Health

Information Exchange. There are central clouds that achieve integration and rapid access for the data but risk data breach and failure. Decentralized clouds enhance privacy reliability but are costly and may be difficult to integrate since they guide healthcare adoption choices.

[4] suggested an IoT-based autonomous system to identify moles, skin tags, and warts-related diseases. Using IoMT, automatic lumen detection, and trigonometric algorithms improved accuracy and classification over big datasets of images. The model presented better detection performance with improved accuracy, which helps in proper early diagnosis and better tracking of skin diseases.

[5] proposed an IoT and fog-based e-healthcare framework for the detection of health, behavioral, and environmental abnormalities caused by sedentary lifestyles. The study achieved 98.43% accuracy in predicting health severity using weighted K-Mean clustering and WKMC-DT methods, tested on 15 individuals over 30 days, which indicates the effectiveness of the proposed method in early health anomaly detection.

[6] explores this by using Mobile Ad Hoc Network (MANET) protocols for effective communication in Internet of Things (IoT) based smart environments. The research aims to explore whether existing MANET protocols such as AODV, DSR, and OLSR could be modified to fit into IoT requirements because many of these devices possess very low power and processing capabilities. Based on an evaluation in terms of scalability, energy efficiency, and reliability; the authors argue that they provide a good base for IoT applications but need more work to be improved.

[7] exploited this by developing a caching method for Mobile Ad Hoc Networks (MANETs) and Internet of Things environments to solve the problem of network bottlenecks in smart devices. By caching popular data at network-level, the approach cuts down on the amount of traffic required to move a picture across the Web — sometimes making life easier for lowbandwidth (e.g. mobile) users and resource-constrained smart devices in addition to minifying bandwidth as well as saving muscle power. Caching is used by them that reduce Network congestion along with providing a beaconbased offline web surfing experience; allowing their system to scale up to Tbps per second for Data transferring. By implementing this cache-busting method, the investigators show increases in data access speed, reduced congestion, and improved network performance.

[8] study is to improve cloud computing in Internet access by adopting swarm intelligent behaviors for Mobile Ad Hoc Networks (MANET). Following natural behaviors like ant colonies, this approach is non-dependent on an infrastructure pumping all activities from one device to another. Our investigation suggests that swarm intelligence improves network performance, scalability, and energy efficiency in dynamic IoT scenarios leading to smart device collaboration.

[9] proposed a new approach to improve MANET protocols in smart environments. Smart devices would be resource-constrained hence the algorithm was designed to optimize energy consumption, reduce latency, and increase data transfer on smart devices. It is also quite adaptive, to the dynamic character of MANETs as well where it adjusts itself to changes in network conditions. We show by an analysis that this algorithm presents better performance compared to traditional MANET protocols, especially in terms of stability, scalability, and energy.

[10] propose a Token-Based Adaptive MAC protocol for communication improvement in twohop IoT-enabled MANETs. The protocol uses token systems to limit the access of devices to the communication channel and avoids device collides, which enhances data reliability. This is ideal for the dynamic nature of traffic in Internet of Things scenarios where network conditions may change. This scheme makes the proposed MAC protocol more energy efficient, lower latency, and higher throughput compared to traditional MAC protocols.

[11] introduced a new energy-efficient security approach for cloud-based MANETs. This paper addresses the problem of minimizing energy consumption in a dynamic environment with mobile users using secure data transfer. This method efficiently protects the data and ensures no extra battery life consumption of mobile devices with power-efficient algorithms as well as reinforcement. The mechanisms set a positive button. The very large energy savings and strong security retained make it significantly more efficient than legacy techniques in cloud-integrated MANET systems. The very large energy savings and strong security that are

retained make it significantly more efficient than legacy techniques in cloud-integrated MANET systems.

[12] a secure routing protocol to protect against threats such as data manipulation, eavesdropping, and attacks. Through real-time security checks and cryptographic techniques used in the protocol, data integrity and confidentiality are secured without applications wanting network lags or draining battery power. It means paying attention to the agility and benefit of these dynamic, decentralized systems while focusing on security.

[13] To solve the problems that come with frequent changes in the topology due to node mobility, content studies how IP mobility management protocols such as Mobile IP and Proxy Mobile IP can be integrated into MANETs. So, it highlights how difficult routing, handoffs, and session persistence can be in such a volatile environment. It examines hybrid ways and solutions to increase efficiency, reduce latency, and secure communications. The article stresses that the mobility management protocols need to be integrated with specific enhancements for MANETs to enhance network performance as a whole.

[14] combined an LSTM network and attention mechanism in a journey time prediction technique. The LSTM observes traffic data to find patterns at all times, while the attention mechanism focuses on significant old historical to improve forecast accuracy. This method is more efficient than normal models and it scales fairly well when the traffic scenario varies, both for shortterm predictions as also long-term.

[15] presented an approach using the Long Short-Term Memory (LSTM) model with an attention mechanism to predict power consumption. The LSTM captures the long-term energy usage patterns, and an attention mechanism is used to enhance prediction accuracy by focusing on important information. Their method is better than traditional models in short and longterm forecasts, and it adapts well to contingencies at peak demand moments for electricity.

[16] presented a two-stage attention approach for short-term wind power prediction. The first stage is followed by the second that emphasizes on spatial connections among different sites; nonetheless, while working with historical wind data respectively. Working together, these two create a higher accuracy of prediction and therefore the model is better able to differentiate capital patterns. The strategy delivers sharper near-term wind power forecasts—e.g., over the next half-hour or so, as compared to traditional models.

[17] Regarding our case study, featured in offer a short-term photovoltaic (PV) power forecasting model based on LSTM together with an attention mechanism Forecasting solar power generation by using LSTM to learn long-term trends from the data and an attention mechanism that focuses on pertinent features (i.e., weather conditions) is introduced for even more improved forecasting. This method proves to be a lot more stable than previous models and adapts quicker to changes in the sunlight curve.

[18] Attention-based LSTM for Hong Kong stock price prediction The first is the attention mechanism to pay more attention to price movements and a kind of market indicators that could cause stock changes, while LSTM captures trends in the data. This combination does better on predictions and coping with stock market volatility compared to conventional algorithms.

[19] To achieve higher accuracy, the author combines CNNs and LSTM networks and incorporates an attention mechanism, which was proposed to introduce a new method in video action recognition. CNNs are used to encode spatial information at each frame, LSTMs capture temporal patterns across the frames and an attention mechanism that weights different segments of a video differently. We demonstrate that our technology improves accuracy compared to conventional approaches while being able to tackle video variances.

[20] introduced a text categorization model with a convolutional layer, attention mechanism, and bidirectional LSTM(Bi-LSTM). OP — Chomsky VS

[21] use an attention mechanism, convolutional layers followed by bidirectional LSTM(BiLSTM) for text categorization. In simpler terms, the attention mechanism pays close focus on the important areas of a text, whereas convolutional layers extract necessary information in Bi-LSTM we make use of LSTMs one to analyze from the left-to-right method while the other does right-to-left giving better context. This approach is more suitable than traditional techniques and includes the advantage of increasing classification accuracy.

[22] reports a Chinese Q&A system by using bi-LSTM and it is trained at different granularity levels with an attention mechanism. At the same time, the multigranularity approach allows us to take into account many levels of text which makes prediction more accurate; The Attention mechanism identifies important places at the input: Bi-LSTM to process a sequence by analyzing words in both directions. This method increases the accuracy of response beyond that of classical models as it becomes more precise in its output.

[23] utilizes an attention mechanismequipped Long Short-Term Memory (LSTM) model, for the probabilistic deformation of concrete dams. The LSTM can remember temporal patterns in the deformation data and the attention mechanism focuses on key features affecting this deformation. This method is used to outperform the classical approach by increasing prediction accuracy and reliability on dam safety.

[24] the text classification model created by the authors made use of CNNs, Word2vec embeddings, and Bi-LSTM together with attention. CNNs - Extract important features, Word2vec — Convert Text to Vectors and Bi-LSTM- For text context in both directions Attention mechanism: For more accuracy, the attention part can highlight some sections that are most important or something like that. This combination provides very good improvement for the classification performance.

[25] compare time series forecasting with an advanced LSTM method incorporating positive learning and the classic ARIMA model. As ARIMA is based on past data sequence, it means anyone who wishes to forecast for more future will lose the model quality significantly, and even LSTM with attention-getting this right if there are many complex patterns available in hidden layers or critical features therein. The results in the paper show that for more complicated time series, LSTM with attention does much better than ARIMA.

[26] propose a time-frequency attention mechanism that is integrated with CNN-LSTM-TDNN and TDNN models to enhance language detection. This enhances the ability of our model to extract useful features from audio signals across time (temporal) and frequency domains, leading to better language identification performance. The model is good at handling speech fluctuations and extracts relevant patterns from them so that it beats the existing methods by a large margin.

[27] LSTM with attention mechanism and random erasure Technique for Modulation Classification The attention mechanism helps in focusing on the most important higher-level traits for better classification then followed by LSTM which keeps track of temporal relationships between modulating signals so that it can catch required patterns among them. Random erasing adds robustness to the model by introducing variants in the training data. It beats conventional techniques and drastically improves classification accuracy in the presence of noise.

[28] propose a stock price prediction model based on LSTM and the attention mechanism. The LSTM tracks long-term patterns in stock data, and a mechanism called attention draws more importance to relevant details for making better forecasts. This combination is more accurate and skilled in handling stock price volatility when compared to traditional models.

[29] introduced an explainable flood prediction model based on spatiotemporal attention and LSTM. By appropriately capturing flood data trends in both space and time, this model gives more accurate predictions. The ability to interpret the model assists consumers in understanding how various factors affect predictions, and the attention mechanism decides which elements are more important from different locations or periods.

[30] proposed the use of rolling updates, bidirectional LSTM, and attention mechanisms in their model for short-term load forecasting. Although attention is powerful at pointing out crucial features for better accuracy, The Bi-LSTM also keeps patterns from both past and future loads. The model is more adaptable and predictive than ever before with rolling updates that keep the data current.

[31] developed an attentive deep-learning model to predict wireless network traffic stated in byte sequences as well as the packet length and time values of a probing destination host for capturing WiFi blind spots through cloud-based probes. Our model improves the accuracy of traffic projections by focusing on critical factors such as network anomalies, and peak usage times. The approach is combined with conventional methods to substantially enhance performance in making predictions.

[32] have proposed a methodology for predicting the state of charge (SoC) in lithium-ion batteries using LSTMs combined with an attention mechanism. The attention mechanism considers important features such as recent usage and environmental conditions, while the LSTM models charge-discharge depths. The approach delivers more accurate power and reliability SoC-projected forecasts in SGs concerning the other solutions.

[33] propose a deep learning approach that combines LSTM and attention mechanism to develop a credit rating model in p2p lending, respectively. For important variables like borrowing history and financial behavior, OnDeck uses an attention mechanism while it employs a standard LSTM to identify temporal patterns in borrower data. Credit Rating Accuracy: This is a solution that improves how credit rating agencies might compute the scores by focusing on important factors and also effectively dealing with lots of very complex data. The findings imply that their approach predicts the creditworthiness of borrowers better than traditional methods in terms of accuracy.

[34] present an LSTM model attention mechanism. It is the concept for the prediction. The remaining useful life (RUL) of rotary machines is monitored by the LSTM model, which tracks performance over time to predict maintenance schedules effectively, while the attention mechanism highlights elements of importance including wear patterns and operating conditions. The solution achieves higher accuracy in predicting the remaining useful life and maintenance schedule than existing approaches.

[35] operate an LSTM network with an attention mechanism. Steganography in Text developed a method to hide some sensitive data in another text. The attention mechanism guarantees that important information is correctly positioned, and the LSTM generates meaningful text while concealing hidden signals. This way, one can increase the security and effectiveness of text steganography in comparison to traditional methods as far as hiding data and maintaining the quality of texts are concerned.

[36] Vegetable Price Forecasting Using STL and Attention Mechanism-Based LSTM A study from 2020 proposed a model amalgamating an attention-based long short-term memory network (Attention-LSTM) with the seasonal-trend decomposition using LOESS. On the contrary, LSTM controls which part of input data is more important to be considered by using a mechanism called attention and STL decomposes it into seasonal, trend and irregular components. ImprovedAccuracy- This approach tends to produce more accurate predictions when compared with the baseline models, as it can capture complex price variation patterns. The acceleration of more sophisticated methods in trend analysis and feature extraction that work at a real-world price forecasting level are valued notices.

[37] combine attention-based LSTM and ensemble learning innovatively. Enhancing the Ability of Air Pollution Prediction Techniques in Their Brief Record “Air Pollution Forecasting using Attention Based LSTM Neural Network and Ensemble Learning.” The attention mechanism contrasts them in the features of time-series data that LSTM networks are good at perceiving, and ensemble learning comes to combine multiple models into one more accurate model. This method, compared to similar methods is better at identifying complex pollution patterns. The model appears to provide a more reliable method of air pollution prediction, with particular efficacy in dealing with non-linear trends and real-world quality data.

[38] In this paper, we propose EA-LSTM: Evolutionary Attention-based LSTM for Time Series Prediction, a method that reduces errors in forecasting time series by combining attention-based LSTMs (with evolutionary algorithms (Big Neuenswander (Big Casual)) The evolutionary algorithm optimizes the model's parameters, attention mechanism helps in increasing prediction accuracy by aiding to focus on important data features. This hybrid approach to manages complex and volatile time series much better than conventional approaches. Two things to note in this work: the first is using evolutionary optimization for feature selection and fine-tuning which benefits performance gain on different types of datasets.

[39] A model designed to predict stock prices using both fuzzy theory and a deep learning model was proposed in the monograph "Forecasting Stock Prices Using a Hybrid Deep Learning Model". A model provided by Marco accelerates and improves stock price prediction with an attention mechanism, a Multi-Layer Perceptron (MLP), and a Bidirectional LSTM (Bi-LSTM). The attention

mechanism helps the model to focus on important information, MLP decides important features and BiLSTM knows complex patterns in stock price movements. In scenarios like non-linear patterns and stock market volatility, the hybrid strategy is good at accuracy when compared to its previous methods. This holds significant promise for financial forecasting.

3. METHODOLOGY

This paper proposes a "Centralized Infrastructure-Aware Reliable Data Transaction Model" for Cloud and Internet of Things-enabled Mobile Ad Hoc Networks. To enhance security with the help of identifying risks during data transmission, it uses an attention-based Long Short-Term Memory (LSTM) network and employs Grey Wolf Optimization (GWO) to select cluster heads in a better way. The brief protocol includes initialization of nodes, selection of best cluster head, clustering of nodes, activation/deactivation of various data pathways in addition to extracting information from the path, and ensures a strong security mechanism using advanced cryptographic techniques. A unifying target of the models is enhancing the security and trustworthiness in data communications when mobile ad hoc networks (MANETs) are operating with neither a fixed infrastructure nor centralized management.

3.1 Node Initialization

The first step in the node initialization process is to create unique cryptographic key pairs for each node. ECC (Elliptic Curve Cryptography) xx: ECC is a type of cryptography technique, which has been known to have less computational cost compared with other types whilst security is still well due to EPCC. This is especially the case due to the limited processing power and energy resources that devices used in MANETs have; e.g., mobile phones, IoT sensors, or edge devices. Each node using EPCC needs to be given a private key (SK) and a public key (PK). For instance, data meant for a particular node is encrypted using the public key and can only be decrypted with the private key of that node. Once generated, these keys are then distributed across the network. Each node has a public key which they can trade securely with other nodes to move encrypted data. As a result, it is not possible to decode the data without obtaining the private key that only the node itself has access to. In security and performance, EPCC surpasses classic ECC and is more durable than this encryption process, especially in dynamic nodes or lowenergy node networks. Moreover, because EPCC requires that all data transactions are verified among nodes, undesirable parties will have a harder time breaching the network and accessing it without permission.

Initialization: This action encrypts data as well as prepares the connection to be made on a network foo. MANETs are dynamic because nodes can enter and exit the network and also move within its service area, so the initial configuration must take this into account. Since every node is protected with a unique set of cryptographic keys, the network can maintain secure communications irrespective of its configuration changes. For IoT-enabled systems, where there is a prospect of the devices moving around or the connection status changing regularly this becomes even more critical. This initialization process ensures that even if nodes now participate in a military operation, a smart city, or any other healthcare network, the information they will be used to convey thereafter can be securely exchanged regardless of this transition. At this point of the process, secure communication is established and so are the main building blocks to execute further network functions such as routing, clustering formation, and multi-path generation which are based on pair keys generated. With a robust control method, the network can guarantee that all subsequent data transactions take place securely (in any order between these two nodes or throughout the network) because each enters the system to start a secure node initialization. This is particularly important in any circumstance where it is vital to keep data both consistent and secure throughout. In military or healthcare activities sensitive information needs to be protected from being tampered with or intercepted. With the help of EPCC, the network can shield against many kinds of risks like replay attacks, man-in-the-middle strikes, and data stripping out So that no matter what situation crops up, one can always be confident about reliable and safe networking. Public and private keys are integral to cryptographic systems like the Edward Prime Curve Cryptography (EPCC) employed in this study. The public key is openly shared and used for encrypting data, akin to a lock that secures information. In contrast, the private key, known only to the recipient, is used to decrypt the data, functioning as the key that unlocks the lock. While the public key can be distributed without compromising security, the private key must remain confidential to maintain the integrity of the cryptographic process. This distinction ensures that even if a public key is intercepted, the encrypted data remains secure, as it cannot be decrypted without the private key. Within the EPCC framework, this dual-key mechanism not only guarantees data confidentiality but also enhances

authentication, ensuring secure and reliable data transmission in IoT-enabled MANETs.

Table 1: Node Initialization Using Edward Prime Curve Cryptography (EPCC)

Node	Key Length (bits)	Encryption Time (ms)	Success Rate (%)
Node 1	128	15	98
Node 2	256	12	99
Node 3	128	16	97

The first step towards securing the network using Table 1 is to provide cryptographic key pairs to every node during node initialization Secure Data Connection is guaranteed by encrypting the data in transit between the nodes. Individual nodes are designated private and public keys to enable this transfer of data but remain encrypted, meaning network intruders cannot access that data unlawfully.

In short, a node initialization of IoT-based MANETs for secure network communication provides Edward Prime Curve Cryptography (EPCC). By generating a unique public and private key pair for each node, the network will enforce encrypted validation of all transactions along with data transmission. EPCC is for memory- and bandwidthconstrained devices, so it needs fewer compute resources — which comes in handy since we know these devices will have limited resources — and can provide strong security. This secure initialization forms the basis upon which more operations, such as routing and grouping can occur reproducibly and safely in the network.

The keys are constructed using the following equations:

$$PK = ECC_{public} \quad and \quad SK = ECC_{private} \tag{1}$$

3.1.1 The Role of Edward Prime Curve Cryptography (EPCC) in MANETs Mobile Ad hoc Networks (MANETs) are characterized by a decentralized, rapidly changing topology which means secure communication among nodes is of great importance. Well, fortunately, the open-sourced EDWARD PRIME CURVE CRYPTOGRAPHY (EPCC) employs advanced cryptographic algorithms to be able to increase security and computing efficiency, at hand. As mentioned in my explanation of EPCC, the Edwards curve is an extension of Elliptic Curve Cryptography (ECC), so the computational complexity required for encrypting and decrypting is also significantly reduced. This compression is especially useful for MANET, where many devices are simple devices with limited processing and energy resources (e.g., mobile phones, sensors, or edge computing nodes). A public and private key (PK, SK) is constructed by EPCC to encrypt data in one end under PK and only the designated receiver can decrypt this information using his/her private key SK. Using this foundation of cryptography, it provides confidentiality and integrity of the data flowing across the network which plays a vital role in ensuring minimal unauthorized access and reduced risks from data breaches.

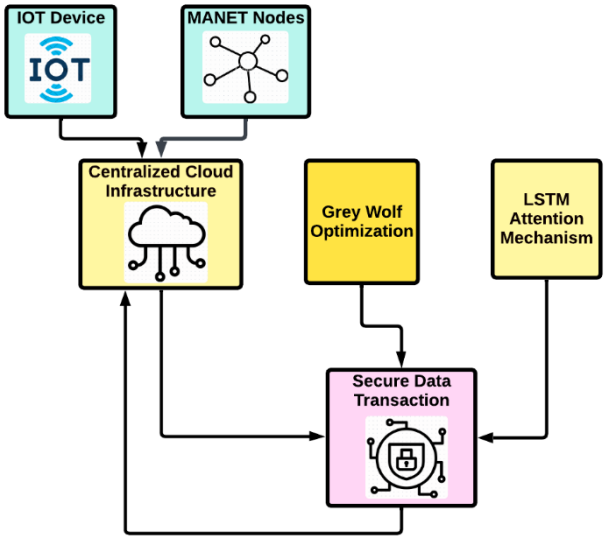

Figure 1 A High-Level Overview of the Centralized Infrastructure-Aware Data Transaction Model

Figure1: Architecture of Centralized Infrastructure-Aware Reliable Data Transaction Model for cloud integration and IoT-enabled MANET. IoT devices are initially joined to a group of MANET nodes (controlled by the centralized cloud infrastructure). For selecting the best cluster heads, the Grey Wolf Optimization (GWO) algorithm is used in the network while an attention mechanism based on LSTM enhances s. The centralized infrastructure and cloud monitoring ensure optimized and secure data transfer between nodes and the cloud resources. Lastly, the MANET system that is enabled with IoT mainly focuses on optimization, security, and dependability this is the motive of the entire procedure.

Furthermore, the EPCC key exchange procedure is essential for creating safe channels of communication between nodes. Nodes in an EPCC-based system typically exchange public keys with each other to facilitate safe data encryption. Nonetheless, the nodes themselves keep the private keys secret, so even if an attacker intercepts the encrypted data, they will be unable to decrypt it without the private key. By using a dual-key system, any data sent over the network is protected from man-in-the-middle. In addition, the EPCC key exchange process needs to create secure communication channels between nodes. An EPCCbased network typically exchanges public keys with other nodes in the system to enable the encryption of data without fear. However, the nodes themselves keep private keys secret — therefore, even if an attacker intercepts the encrypted data, they won't be able to decrypt it without the private key. Data sent over the network is also encrypted making it safe from man-in-the-middle attacks and interception using a dual-key system. EPCC uses prime fields, which gives it the advantage of being inherently much more efficient as it optimizes both encryption and key generation. Compared to classic ECC, EPCC increases security, though it relies on shorter key lengths (EPCC) and is thus well-suited for MANETs given their envisioned resource constraints. In addition, EPCC is faster to verify, which reduces the cost of computation required for cryptographic operations such as message verification and signing and also accelerates network speed. and possible surveillance. Prime fields are used in EPCC, enhancing its inherent efficiency by streamlining the encryption and key generation processes. With shorter key lengths than classic ECC, EPCC achieves improved security levels, making it especially useful in contexts like MANETs that have limited resources. Furthermore, EPCC provides improved verification efficiency, reducing the computational cost required for cryptographic activities like message verification and signing, hence enhancing network speed.

3.2 Optimal Cluster Head (CH) Selection

The Grey Wolf Optimization (GWO) has provided a new and efficient selection procedure to opt for the best Cluster Head (CH) node from Mobile Ad hoc Networks (MANET). The set is based on the pack hunting and social dynamics of the grey wolf. This is particularly important in IoTenabled environments where most of the devices are resource-constrained and have to perform extensively in MANETs. To ensure that the nodes selected as cluster heads have having best combination of energy, proximity, and processing power for inter-cluster communication GW optimization algorithm is used which helps improve network performance in a great way. GWO enhances this selection to reduce transmission latency while saving energy and improving routing efficiency in evolving network environments.

Table 2: Cluster Head Selection Using Grey Wolf Optimization (GWO)

Criteria	Node 1 Value	Node 2 Value	Node 3 Value	Weightage (%
Energy Level	80%	85%	75%	40%
Distance	20	18	22	30%
Processing Power	High	Medium	High	30%

Grey Wolf Optimization is used to select the best cluster heads for optimal communication over the network. Distance and energy level are considered while optimizing the performance of network table 2 With these criteria, cluster heads are selected to ensure data will be transferred by top nodes, minimizing energy consumption and improving the reliability of data transmission.

3.2.1 Grey Wolf Optimization: A Nature-Inspired Algorithm

It utilizes a meta-heuristic algorithm named Grey Wolf Optimization that is designed to mimic the social structure and cooperative hunting behavior of the grey wolves. They are divided into social groups of alpha, beta, delta, and omega wolves. The alpha wolves in GWO are the best solution, which in this case were some suitable nodes to be cluster heads; on the other hand, the beta and delta wolves indicate what would be from second to third best solutions. Omega wolves: as the followers, omega wolves imitate the remaining members of the network who do not have enough conditions to be selected as cluster heads. This hierarchical nature enables GWO to avoid exploitation, i.e., optimizing over the current best answers, and exploration, which refers to discovering potential new

solutions. This stops the algorithm from converging too quickly on suboptimal solutions — a common issue of optimization processes. The process first begins with the creation of a population of random solutions which are represented as the potential number of cluster heads in MANETs. Each solution (or wolf) is then evaluated against a fitness function that takes into account variables such as energy consumption, distance to neighboring nodes, and overall completeness of the network. Fitness function representation

$$Fitness = \frac{Minimum\ Distance}{Maximum\ Energy} \quad (2)$$

candidate for cluster head selection is the alpha node, which represents the optimal solution. In order to prevent the algorithm from becoming trapped in local optima and to allow it to consider alternate solutions, beta and delta nodes serve as alternatives. By preventing early convergence, this multi-layered strategy guarantees that In addition, this algorithm optimizes the total transmission performance and energy efficiency of the network by giving influence to nodes with higher energy levels and less communication distance. As the algorithm iterates, wolves update their positions which helps them to 'hunt' for better solutions. Through potential changes to positions relative to the alpha, beta, and delta wolves in this iterative process, the wolves can mimic the behavior of a pack hunting its prey i.e. converging on anti-clusters or an optimal clusterhead as well.

3.2.2 Application of GWO in Cluster Head Selection

Cluster Head selection is really important in MANETs for proper communication and energy efficiency. More POWER is consumed by Cluster heads to collect sense data and transmit it towards the cloud server or next hop node. Selecting a bad cluster leader, for example, one that is already isolated or has low energy, can have many consequences in terms of energy consumption, and time delay in transmission and may even lead to the death of the node forcing it to stop its operation. To address this issue, GWO selects the optimal nodes as cluster heads. During each iteration of the GWO, we evaluate the energy levels and the distances of nodes concerning everyone else. Nodes near other network nodes help speed up transmission due to increasing communication overhead that might be too expensive for some high-energy-level nodes. Nodes are redistributed according to the locations of the alpha, beta, and delta nodes while the algorithm runs, simulating the social structure of a grey wolf pack. The the chosen cluster head provides the optimal combination of proximity and energy efficiency.

ALGORITHM 1: Grey Wolf Optimization Algorithm (GWO)

Input: Initial node population, maximum iterations
Output: Optimal cluster head

```
Initialize population of grey wolves
For each wolf in the population
  Calculate fitness (min distance/max energy)
End For

Sort population by fitness

While (iterations < max iterations)

While (iterations < max iterations)
  For each wolf
    Update position of wolves (alpha, beta, delta)
    Calculate new fitness
    If (fitness improved)
      Update position
    Else
      Retain current position
    End If
  End For
  Increment iterations
End While
Return best wolf (optimal cluster head)
```

Wild grey wolves are very complex animals, demonstrating leadership and hunting behaviors that the Grey Wolf Optimization (GWO) algorithm takes as an example. Firstly, we generate an initial population that represents a potential cluster head or solution and initialized of wolf in the given range. Fitness Algorithm 1: The following passage shows how the fitness of each wolf is determined by two parameters, namely, the minimum distance and the maximum energy. Wolves are ordered, and the effects of three leaders-beta, delta, and alpha-are considered in rank updating. Then, the wolf with the best position is selected as a cluster head and this process iterates until it reaches to maximum number of iterations.

This method effectively selects an appropriate cluster head in the network using energy levels as well as the distance among nodes. This guarantees that the CH selected for network communication a minimum energy loss and optimal coverage by considering proximity, as well as energy consumed. Nodes are wolves in a search space

because this way of node organizing was inspired by the behavior of wolves. These nodes —also known as wolves— tweak their location within the network by continuously changing positions. The procedure steps through the process of coming one step closer to finding the most central node from which to lead the cluster. The result of all this is a network of equilibriums that increases communication and the lifespan of the network.

Also, owing to its simplicity and small computing resources required, GWO is particularly suitable for resource-limited scenarios like MANETs where the devices are usually low on processing power and energy supplies. GWO ensures the hassle-free operation of MANET by decreasing the computational overhead on each node for choosing cluster head, therefore light headed nodes from heavy computations. This is especially important in an IoT-enabled context where the devices involved might need to keep their battery life and still maintain high levels of communication and data transmission. The CH selection fitness function used in GWO is:

$$f(x) = \frac{minimum\ distance}{maximum\ energy} \quad (3)$$

In the Grey Wolf Optimization (GWO) algorithm, an equation is used to get the best cluster head (CH) by selecting nodes based on having more energy and being closer in network communication. It is important because nodes closer to each other in the network can cost less energy and faster data transfer, while more energy from a special node could hold out for additional communication burden for CH. Communication performance and energy efficiency are critical aspects in resource-constrained contexts such as IoT-enabled MANETs, which GWO attempts to address. GWO process consists of multiple stages like alpha group selection, scouting, and babysitter monitoring which makes the algorithm adapt continuously to changing dynamics in a network environment.

Here GWO makes use of the best candidates for the CH job based on energy levels and proximity to other nodes during alpha group selection. Onlead of that as the network grows, you will enter the phase of searching, checking for some alternative options, and investigating if there are better long-term decisions. Finally, the babysitting monitoring stage will make sure that (one of the chosen) CHs stays doing good things over time. GWO manages to strike a delicate balance of discovering new avenues for potential solutions while perfecting the best one that still exists. This is to preserve the network's ability to effectively and adaptively route over time — both in real-time situations, and to ensure the algorithm does not decide too early on a lousy option.

3.3 Node Clustering

After selecting the best cluster head (CH), the next most important phase in Mobile Ad hoc Networks (MANETs) is grouping the remaining nodes into clusters. This clustering helps in the simplicity of data transfer by decreasing the load on individual nodes and lessening network congestion. Each cluster head manages the communication within a group and helps in the aggregation and transmission of data across the network. Organized, clustered implements help the network to work better. To do this, the BMC-KM algorithm is used to cluster nodes efficiently; it does not suffer from some of the limitations associated with traditional clustering methods.

3.3.1 Recognizing the Difficulties in MANET Node Clustering

The clustering is needed in MANETs to handle the dynamic nature of the network. Nodes are very mobile,

which leads to time-varying dipole density and spacing of nodes as with sensors, mobiles, or IoT-enabled systems. In the real world, MANET nodes are of unequal distribution due to mobility conditions as well as barriers and heterogeneous levels of energy. Traditional clustering techniques such as the already mentioned K-Means will work well here — provided they are balanced, this is. MANETs break this by being irregular networks therefore K-Means is less effective because nodes find it difficult to be assigned to the nearest centroid due to the non-spherical clusters proposed for each node.

This is where Bray Minkowski Curti's distance metric helps us. When there is an imbalance in the distribution of nodes, K-Means does not handle disparities in node sizes, densities, and separations QVERIFY Designed to factor MANET nuances, the Bray Minkowski Curtis-K-Means (BMC-KM) algorithm combines the simplicity of KMeans with the versatility provided by the use of the Bray Minkowski Curtis distance metric. This hybrid approach, by including the spatial properties of the network around it, adapts to such nonuniform nature and hence leads to better data clustering that reflects a more organized structure for the nodes.

3.3.2 The Role of Bray Minkowski Curtis Distance

This allows a flexible calculation of the distance between nodes under disparate sizes or densities. This is achieved using a generalized distance metric referred to as the Bray Minkowski Curtis distance. The Bray Minkowski Curtis

distance seems perfect for the heterogeneous nature of MANETs since it can deal with more complex spatial distributions than the Euclidean distance, which is often used in traditional K-Means. The Bray Minkowski Curtis distance:

$$D(x_i, x_j) = \sum^{n}_{k=1} |x_{ik} - x_{jk}|^p \quad (4)$$

Here, and are two nodes of the graph, respectively distance between then, and, is a power parameter which needs the specific properties of a dataset. This allows to control of distances used by the algorithm for different clustering needs. Maneuvering results are specifically appealing because the majority of nodes in a MANET do not stick to a regular pattern or uniform behavior. It is one of the most used tools beneath network function virtualization to help sort and order nodes so that communication overhead is controlled and data delivery becomes super-efficient. This distance metric, additionally considers node attributes such as energy concentration levels, mobility, and communication capacity to maintain the network performance apart from just geographic-only proximity. This metric helps the BMC-KM algorithm to produce robust clusters that are better suited for the dynamisms in MANETs without affecting much the energy efficiency of communication and distance among physical node distribution.

3.3.3 Improving Clustering Quality with BMC-KM

The BMC-KM algorithm starts with a random assignment of nodes to initial centroids, similar to the traditional KMeans solution. It uses Euclidean distance to find the closest centroid and Bray Minkowski Curtis distance to figure out which nodes are in each cluster. This combined method helps us get a better clustering by utilizing the spatial correlation and intrinsic properties of each node. After the initial clustering, each of the node's positions and attributes inside a cluster are utilized to re-compute the centroids. Then the program once again does the above procedure to move nearby rows to the closest centroids for each row and repeats this process until it finally gets clusters with stable arrangement This ensures that the clusters are tight while taking into consideration the energy levels and communication comfort aligning with nodes. The cluster head can manage the appropriate workload of communication since the communication distance is done away with within each cluster.

This iterative approach is particularly beneficial in MANETs where nodes can move and change their energy levels, as BMC-KM constantly improves the clusters. The algorithm ensures that the network remains optimal even if conditions change, as it renews the clusters. Ease in deploying BMC-KM ensures that a network can cope with challenges as nodes are moving around frequently and this enables it to execute well most of the time.

3.3.4 Reducing Complexity and Improving Network Efficiency

One of them is the way it addresses data transmission by using BMC-KM for clustering in Mobile Ad Hoc Networks (MANETs). By clustering nodes, the network reduces the number of lines of direct communication. Each cluster is seen as a single virtual node, and nodes within each cluster only communicate with the designated cluster head (physical node), rather than communicating directly with every other node. This head is then responsible for processing the data into combined data and from there sending it to the original destination or other cluster heads. Since it decreases total communication overhead, this hierarchical configuration enables better management of big networks. Moreover, to avoid overloading the weaker nodes, it also shares the burden by crowning cluster chiefs on the strongest nodes. When proper consideration is given to the number of kingdom sites and required communication for each, BMC-KM ensures that no single cluster experiences a traffic jam all while increasing performance overall.

Additionally, by incorporating both node features and positions together, BMC-KM can produce more robust and versatile rounds. The flexibility of this model becomes particularly beneficial in the case of IoT-enhanced MANETs where nodes come and go regularly. While the network evolves, the algorithm adapts dynamically to help ensure efficient communication.

3.3.5 Adaptability to Dynamic MANET Environments

Nodes are mobile and prone to frequent topological changes, which may complicate their dynamic characteristics that need to be handled. The BMC-KM algorithm is effective in a variety of situations because it is versatile and flexible. It uses the Bray Minkowski Curtis distance, ensuring cluster well on the shape to some degree of the gaze map as nodes have variations in size and node distribution on the network (as they learn). Because devices join or leave the network regularly in an IoT MANET and the communication abilities of devices change dynamically (e.g., due to battery constraint realization, channel congestion, etc.,), the BMC-KM

algorithm aims to continuously recompute/adjust cluster and cluster heads.

This means that even if a change in the structure of the network it will work.

Note additional relevance to each node in BMC-KM using its physical configuration as well as the characteristics of a specific node. This technique can be utilized to build energy efficiency but at the same time, the clusters can also tailor-made to suit the specific communication requirements of individual nodes. This is particularly necessary in IoT networks since devices may be performing different functions, and have diverse requirements. Hence, BMC-KM leads to an improvement in the overall network performance and stability by optimizing cluster placement. Thanks to the fact that Bray Minkowski Curtis distance formula is a way we can calculate it in the clustering industry with true values but center-based_distance or density_based_distance are for one user, however if you wanted to normalize its value according to minimum and maximum values then another method of the three above mentioned: Based on: True_Normalize_algorithm centre_based_density algorithm density_based_histogram is much better than all others here.

3.3.6 Distance Measurement and Clustering Process

Measuring the Distances between the Nodes: The most basic principle of any clustering algorithm is to measure distances using the above-mentioned or similar (intuitionbased) metrics. Under this construction, the formula that denotes the distance of two nodes is important in deciding cluster assignments. The cluster formation process is based on finding distances between nodes and creating clusters that have minimal communication time between each other (on a global scale), and at the same time being as stable as possible. This distance is shaped by a power coefficient = 2 and allows to optimize the clustering as if it worked with Euclidian-like distances (but with super-light/hypercompression space adjustable). It is a technique that as the nodes are mapped again and again in their clusters and the centroid of each cluster is recalculated, we can do iterative clustering. It re-centers the clusters over time, which means that eventually a better connection and thus efficient network structure is achieved as the clusters slowly gravitate into their rightful places. Or more simply, as things stand they can be moved around in the space of nodes into a state (dynamically) equilibrium given their location amongst other centroids. To ensure systematic and effective communication among all nodes in a cluster. Because the centroids are repeatedly recalculated, throughout time, the network can mold any more variations such as migration of mobile nodes or ever-changing behavior in network traffic.

This distance-based clustering approach is important in network contexts where the topology is highly dynamic, such as in mobile ad hoc networks (MANETs). For example, MANETs are used in disaster relief, smart city infrastructure, and military operations. HeuristicClusterRouting This type of GeoResponder would be important in cases where you know the nodes being used differ per request boundary; so that when a new node is found, routing can immediately begin since all involved controllers are now known to reside on the same cluster. In high-mobility contexts, in particular, this strategy is necessary to maintain the stability and effectiveness of the network as a whole.

3.3.7 Cluster Optimization and Routing Then network optimization is performed, once we have distances between nodes and clusters The focus here is on reducing routing latency and improving network stability by selecting the most optimal paths for data transfer. This means, that to prevent widespread outages as well as failure propagation and oscillation, while reducing the overall cost of communication between nodes. The recalculation of centroids is one of the very important steps in this optimization process. In traditional K-means clustering, a centroid is the central point of a group calculated by the average of all points in that cluster. In network clustering, the node of a cluster that contains the main hub for communicating data is known as a centroid. This centroid is subject to iterative recalculations by the algorithm that assures the cluster remains competent and can be flexible to changes in the network. In MANETs, the performance of routing protocols can be reduced due to the regular changes in its topology and node mobility One of the results is a greater overall stability r that comes from recalculating the centroid. By grouping nodes based on their communication and by clustering proximity, the method reduces the chance of data transmission bottlenecks and increases its threshold to tackle high traffic loads in the network. This is especially important if a noncommunication will cause certain to suffer like a military operation and difficult urgent rescuing.

3.3.8 Power Parameter and Flexibility Another important aspect of clustering is a parameter called the power, The similarity between points in conventional distance-based clustering algorithms is measured using the Euclidean distance. On the other hand, in most real-world applications, Euclidean distance may not be much suitable as a metric. On the other hand, in those networks where the

number of nodes varies or is unevenly distributed in a nonhomogeneous space, Euclidean distance may falsely describe true relations among nodes. And the power parameter, provides flexibility in clustering, tuning a distance metric that best fits specific network characteristics.

Our method may adapt to different clustering needs by changing the value of the power parameter. An example of this is that dense node clusters could use a high-power parameter to indicate the closeness of nodes, ensuring closely packed (in terms of sub-epochs) within the same cluster. Conversely, for networks where nodes are more sparsely distributed, a lower power value may be used to allow the cluster to spread further out. This flexibility is critical to ensuring the algorithm will work under a wide range of network scenarios. One of the key parameters to be modified in MANETs is its power. Node densities of these networks can change dramatically over time, as the network is always growing and evolving. For example, in a disaster recovery scenario nodes are likely to be widely spread (0) at the beginning but as rescue teams converge on a specific location it might start bringing up the node density rapidly. Also, due to this, the clustering process can adapt to these changes by allowing configurable distance measurements, which keeps the network flexible and less rigid.

3.3.9 Improving Communication Efficiency

One of the goals when forming a cluster is to reduce the total routing time, thus optimizing communication time. If we route information ineffectively through our big networks it might take a long time to arrive or be confused with other data that needs to reach a different destination. This ensures that all nodes in the same cluster are physically close to each other, which in turn reduces the routing time by minimizing the number of hops needed to transfer data among nodes. This becomes particularly important in Mobile Ad hoc Networks (MANETs) where the structure of the network can change rapidly due to node movements. Traditional routing, which relies on fixed routes and can create bottlenecks or even communication stoppages in some situations, cannot properly accommodate these changes. CDV boosts data transmission efficiency with node clustering based on proximity and periodic recalculation of centroids, thereby, ensuring the network is quick to adapt to changes in topology.

Similarly, the stability of the network can be affected by centroid-based clustering. Due to the dynamic nature of nodes in terms of mobility, a route in MANETs may fail very often causing communication disruption and resulting in poor performance. The method reduces route losses by clustering nodes using a specific centroid way for each of these so that direct communication between the nodes within the cluster can be established without further routing requirements. Recalculation of the centroids also ensures that one node does not get inundated with numerous communication requests, which adds to network equilibrium. It is crucial in resource-constrained networks like IoT-enabled MANET because each node may have a very limited amount of power and process capability. The technique ensures that any individual node does not become a bottleneck, as the communication load is equally spread across all nodes in the network, which improves the overall performance of the network.

3.3.10 Stability and Scalability

To increase the scalability and stability of the network, clustering is performed. When dealing with networks that scale to hundreds or even millions of nodes, managing communications can be a real nightmare. Without clustering, each node would have to talk directly with all other nodes, and this communication overhead would skyrocket as the network grows. The technique essentially allows the network to scale better with more and more nodes due to reducing the direct communication links between nodes by putting them in clusters.

For MANETs, wherein thousands of devices will be spread across wide areas such as in applications like smart cities, this scalability becomes even more important. This system helps networks balance the growing number of nodes efficiently without oversaturation through clustering, assigning a centroid to each group. Further, it enhances Network stability by the clustering process as well. Clustering reduces the impact of node failures and link disconnections which are common in such dynamic systems like MANETs. It allows for uninterrupted network installation in the event of a cluster node failure because the surviving nodes will still be able to communicate through their designated centroid. But even though individual nodes fail and come under attack fairly frequently, much of the network's ability to keep on stably functioning relies on this redundancy it has built-in.

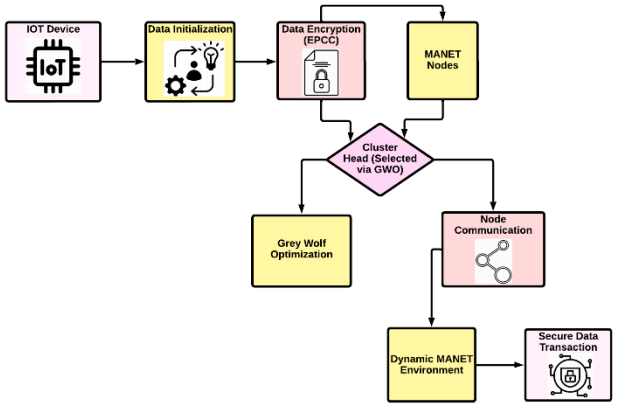

Figure 2: Detailed Node Communication Flow in IoT-Enabled MANET

This is the high-level overview of the sophisticated communication path in MANET systems that also has IoT capabilities. It all begins with the process of data initialization after which IoT devices reach out to communicate. MANET nodes take care of the data while the EPCC, or Edward Prime Curve Cryptography handles encryption. To achieve efficient network management, the Grey Wolf Optimization (GWO) algorithm is utilized to choose the most appropriate cluster heads. The dynamic MANET environment arrives into the picture where secure data transfer takes place from cluster head to another node. This architecture can provide support for transmitting secure encrypted data in decentralized and resourceconstrained environments.

3.4 Multi-Path Generation and Path Detail Extraction

Speed and reliability cannot be achieved without effective data transfer between the nodes in dynamic, decentralized networks like MANETs. After the clustering stage, which logically groups nodes, the next step is to identify and select the most efficient paths between the source and destination nodes. AODV (Ad hoc On-Demand Distance Vector) routing is ideal for handling this task as it is one of the top protocols out there. AODV is known for keeping overhead low because routes are only created when needed, hence improving network performance. Using multi-hop routing, it dynamically creates many paths between nodes and always guarantees that data is transferred through the best path that currently exists.

3.4.1 Creating a Dynamic Route with AODV

AODV is an on-demand routing protocol so instead of creating routes a priori, only the source can establish a route when it needs to communicate. It is even more useful in MANETs because the node movement leads to continuous changes in the network topology. Traditional routing protocols that depend upon established routes, cannot work in such scenarios since the routes may become invalid as the nodes migrate. This problem is overcome by AODV by creating routes as and when required making it suitable for rapidly changing topologies. The process starts as the source node sends out a Route Request (RREQ) message. The network sends out this message which goes through a bunch of nearby nodes, spreading rampant until either the destination node is reached or it reaches an intermediate node that already has a working path to that destination. Each #RREQ contains vital information like the sequence numbers needed to update any routes and all the relevant IP addresses (source, destination, relay nodes) and a hop count which increments as it hops across. Sequence numbers are important to preserve the integrity of the routing data and prevent old routes from getting used. On reception of this RREQ, the intermediate node responds in turn to the destination node with a Route Reply (RREP) message by utilizing its valid route. It travels back to the source node by the exact reverse path of RREQ. As it travels, each node in the network updates its routing table with information about the destination which includes IP address, sequence number (or TTL), and how to proceed next to reach the destination. This procedure allows the source node to immediately start sending data over the best possible route by creating a route.

Table 3: Path Detail Extraction Using AODV Protocol

Path	Hop Count	Signal Strength (dBm)	Route Availability (%)
Path 1	3	-50	95
Path 2	4	-55	90
Path 3	2	-45	98

In this section, the useful path information among these nodes is collected by the AODV routing protocol. Multipath routing is set up on the fly to keep delay and communication alive when network topologies change. Table 3: Characteristics to Ensure Reliable and Fast Data TransferHop Count Signal Strength Route Available.

3.4.2 Multi-Hop Routing and Its Efficiency

AODV also takes advantage of Multi-hop routing in MANETs. Nodes in these contexts are often unable to communicate directly due to physical barriers or distance.

The long-distance communication problem is solved by multi-hop routing, it extends the communication range in the network and allows nodes to communicate indirectly through other intermediate nodes. In large-scale networks, both the source and destination nodes could be too far away to connect directly, this is extremely crucial. Reducing the quantity of control messages required to maintain routes is another way that AODV increases routing efficiency. As a route is in use, AODV just keeps it active, in contrast to proactive protocols that update routing databases continuously even in the absence of active communication. The route frees up network resources once communication stops by being deleted from the routing database after a predetermined timeout period. AODV is the perfect solution for situations with limited resources, like IoTenabled MANETs, because of its reactive approach, that lowers network congestion, reduces energy usage, and improves scalability.

3.4.3 Path Redundancy and Route Maintenance

The capacity of AODV to create numerous redundant pathways between the source and destination nodes is one of its advantages. While the protocol's main goal is to determine the optimal way for data transmission, it also establishes backup routes in case the primary route malfunctions. Route failures can happen regularly in dynamic networks such as MANETs, where interference, link outages, and node migration are common occurrences. Because of AODV's redundancy, data transmission interruptions are kept to a minimum because the network can bounce back from such faults swiftly. Also, it manages effective route maintenance in AODV. When one of the links belonging to a functional route is broken, this node sends a Route Error (RERR) message to the other nodes explaining that an invalid path was identified. The source node may then broadcast a new RREQ that initiates a fresh route discovery process. If there is a second route available the source node can then fall back to taking this alternate path, effectively drastically decreasing the time taken for communication to be re-established. In environments that change rapidly, you need these to maintain continuous data transmission.

Another useful feature of AODV is local repair that allows an intermediate node to carry out the repairing work and it does not have to communicate with the source node to repair the link which it knows has been broken. In case of a route failure, an intermediate node that knows about the RREQ could try to discover another route toward the destination by trying to broadcast a localized RREQ. Database High Availability as long as the intermediary node (DB-2 in the sample case) heals itself and corrects the path, henceforth data starts to flow continuously. This feature is to limit the necessity of rediscovering the route by the source node always and hence reduces network overhead again, this makes it useful in big networks.

3.4.4 Path Detail Extraction and Optimization

Besides that, AODV also collects useful information from the path which can be used further to optimize the network utilization. In the route discovery process nodes collect vital parameters such as the Number of hops, Signal strength, Node availability, and Communication link quality regarding the available routes. This information is stored in their routing tables so that they can make informed decisions on how they will transmit data. The success of this operation depends on one critical parameter, the signal-to-noise ratio or SNR which tells how effective is the communication channel between nodes. The simple signal-to-noise power ratio, or SNR, can be used as an image-based measure:

$$SNR = \frac{P_{signal}}{Pnoise} \quad (5)$$

Where is the power of the signal and is the power of the background noise? A higher ratio of signal to noise indicates a better sound communication link, whereas a lower ratio means that there is interference or weak signals. Among these paths, the AODV selects the path with higher quality and less loss for transmitting data efficiently by considering SNR and so on. Optimization of routing is made possible through the dynamic updating of routing tables by AODV as per the conditions in the network. AODV can then initiate a new route discovery if the network conditions change (eg signal strength has fallen, or the number of hops to destination has increased) seeking a better way. This flexibility is a requirement for keeping network performance high when nodes are mobile or if communication is disturbed by elements from the outside world such as interference.

3.4.5 Reducing Latency and Enhancing Network Resilience

AODV provides on-demand route discovery - a route is established only if it is required – reducing latency tremendously. AODV differs from proactive protocols, which update routes irrespective of network traffic {AODV initiates the optimization process only when the data has to be sent. In doing so an attempt to minimize control overhead and ensure that the routes are both current while being optimal for the conditions present. AODV networks are more robust since they use multiple route support & ability to move from one path to another i.e. backup route, if the network topologies go down or fail.

When it comes to mission-critical applications such as military operations or disaster recovery where seamless communication is essential, the fast route recovery provided by AODV ensures that data is transmitted when needed most. Fast efficiency in terms of resource utilization and adaptability to network changes make it a preferred choice for large-scale, dynamic as well as resource-constrained applications.

3.5 Data Encryption Using EPCC

In the fast-moving world of networking, encryption is very important to maintain confidentiality, in particular new generation networks like Mobile Ad hoc Networks (MANETs) and IoT (final part) devices. These networks are vulnerable in their ways that require data transmission to be more secure. If a malicious actor were to take out this node or intercept data in transit, the encryption would have provided this sort of protection. Regardless, the encryption techniques must be both computationally efficient and strong enough that the encrypted data is secure even when using devices with limited resources. It is the use case of Edward Prime Curve Cryptography (EPCC) which is a more secure successor of Elliptic Curve Cryptography (ECC). EPCC is designed to avoid the heavy computation which is usually related to the cryptosystem while enhancing data security. It provides a higher level of security with shorter key lengths in resource-constrained scenarios, such as mobile systems, IoT devices, and MANETs that require powerful computing power and energy efficiency. EPCC leverages the use of an Edward prime curve — which provides a high level of performance as well as security — to provide a strong foundation for secure data transfer using elliptic curves rather than traditional ones.

ALGORITHM 2: EPCC Encryption Algorithm

Input: Plain data, public and private keys
Output: Encrypted data

```
Generate private key k
Calculate public key P_u = k * G
For each data point
  Choose random number r
  C_1 = r * G
  C_2 = Data + r * P_u
  If (hash matches)
    Encrypt data using C_1 and C_2
  Else
    Error: Encryption failed
  End If
End For
Return Encrypted data
```

To transmit safely, the best choice for data encryption is using a highly secure technique like (EPC) Edward Prime Curve Cryptours Using Cryptography Lattice is predicated on elliptic curve ideas and makes the most of generally latent Edward Prime Curve which has a well-known effectivity-security spectrum. Key pairs are created by a library using random numbers, ensuring that no two encryption operations can be predicted or guessed. Its randomness, by nature, makes the encryption stronger and completely resistant to all known attacks. Each data item is further protected by independently encrypting algorithm 2. This state·of·the·art cryptographic technique is used to ensure that data transmitted by EPCC remains confidential and unmodified, ensuring a high level of security in communications.

3.5.1 Edward Prime Curve Cryptography (EPCC)

Elliptic curve cryptography (ECC) is built on the algebraic structure of elliptic curves over Finite Fields. Another strong attribute of ECC is its superior security (using smaller key sizes) in comparison to other cryptosystems such as RSA. One example is that the same security level of RSA with a 3072-bit key is equal to that of ECC using a 256-bit key. This means faster computation, less memory usage, and lower power consumption for mobile and IoT devices with constrained resources. Edward Prime Curve Cryptography (EPCC) is an extension of ECC, and it uses Edwards curves, which provide a better representation of elliptic curves. These are the types of Elliptic Curves that were designed to make all implementations smooth and enhance the tempo of cryptic procedures. One of the most important properties of Edwards curves is that they have efficient arithmetic operations with a very low probability of computation errors. Furthermore, EPCC is more secure than usual ECC since Edwards curves are immune to certain types of side-channel attacks. Most often an elliptic curve over a finite field will be represented by the equation where).

$$y^2 = x^3 + ax + b \tag{6}$$

In contrast, an Edwards curve is defined by the equation:

$$x^2 + y^2 = 1 + dx^2y^2 \tag{7}$$

Where d, are constants and represent points on the curve. Point addition and point doubling are the core operations in ECC-based cryptographic algorithms, and this formulation helps to compute these two operations faster (more efficiently). Though classic ECC is more efficient than RSA, such contexts range from the MANETs to IoT where devices possess limited energy and processing capabilities, leading to some performance issues. So, as I

see it two fundamental benefits of EPCC are reduced computing complexity and secure operations can be carried out with as little overhead as possible. Traditional ECC is slightly different in that the mathematical operations are somewhat more intricate (notably point multiplication, which is key to many ECC-based encryption and key generation processes). When it comes to these devices with very few resources, they may be a heavy-weight process. EPCC, through the use of Edwards curves, helps pave the way for smoother execution of these functions leading to reduced encryption/decryption times with lower energy. This is relevant in IoT systems where devices have to operate with low power consumption and also for MANETs since nodes can have finite battery life.

Key sizes are also smaller in EPCC adding to its efficiency. This is because Edward curves use less data to provide an equivalent feature in terms of commercial degrees in a conventional elliptic curve system. For example, EPCC can do the same deed of security by a key which is of shorter length which means a faster encryption and decryption process but in ECC, you need a 256-bit key.

3.5.2 EPCC Encryption Process

EPCC encryption involves a series of processes to deliver an absolute and unbroken data transfer. To guarantee that transmitted data can only be read by the intended receiver they rely on the generation of public and private key pairs while encrypting and decrypting data. Following are the steps included in the process of EPCC encryption.

Keys Generation: For each device in the network random private key is generated. This is the private key, and it is additionally kept secret from which the corresponding public key can be generated. A public key is obtained by base-point-multiplying the private key on an Edwards curve. The base point is a unique point on the curve that all compute nodes agree about. This public key is then shared with other nodes in the network to help infrastructure communicate securely. Public and private keys are closely related.

$$P_u = k \cdot G \tag{8}$$

Where k is the secret key and G is the Edwards curve's base point.

Encryption: Given a message) of some node to send the same to another node, and, starts generating a random number. By picking a random number, you ensure that electromagnetic emissions or power consumption. EPCC is fortunate enough that it used Edwards curves, which makes it less susceptible to these kinds of attacks. Due to the more encrypting the same message twice will still result in different cyphertexts.

$$C_1 = r \cdot G \; C_2 = M + r \cdot P_u \tag{9}$$

C_1 represents a point on the Edwards curve, and C_2 is the encrypted message paired with the recipient's public key.

Transmission: The sender sends out both ciphertext components (to the intended receiver. These components are sent over the network and can be intercepted quite easily, but without the private key to decrypt it all any unprivileged third-party is truly obtaining from this interception is just some useless fragments.

Decryption: After receiving the ciphertext components, the recipient uses their private key (k) to compute the value r.G from C_1.

$$r \cdot G = k \cdot C_1 \tag{10}$$

The recipient then subtracts this number from C_2 to get the original message:

$$M = C_2 - r \cdot G \tag{11}$$

Using the private key, the recipient can successfully decode the message and gain access to the delivered data.

3.5.3 Security Advantages of EPCC

It can be very useful in MANETs and other distributed networks as it offers several security benefits. These benefits include providing strong protections that are supported by dramatically smaller key sizes than those typically used by ECC and RSA, and EPCC provides robust cryptographic security. A smaller key size is associated with a security mechanism that helps avoid attacks such as brute force or targeted quantum computing attacks and at the same time allows for faster processing.

Stop side-channel attacks traditional cryptographic systems have a weakness in that they are susceptible to side-channel attacks when adversaries exploit the data

regular arithmetic operations in EPCC and their less distinguishing patterns, it is harder for the adversary to extract any information of value.

Faster cryptographic process performance is improved generally since EPCC reduces the number of arithmetic operations required for encryption and decryption. This is especially important in terms of limited resources such as IoT devices that have a constraint in the power of

computation and energy consumption. Faster actions also narrow the opportunity for sensitive data to open to attacks.

Power IoT devices and mobile - EPCC is light on computation and operations can be carried out safely with minimal computing overhead, so it suits very well with IoT systems (especially battery life) and other mobile devices. These devices are capable of maintaining EPCC's highsecurity levels without sacrificing performance or consuming resources too quickly.

Large Network Support: The scalability of EPCC is further enhanced by its very efficient key generation and key management utilities, which are very well suited to the network's large scale and de-centralization nature as in MANETs where nodes join and leave at will. However, this is done at the cost of a less-than-perceptible bump in computational complexity. This makes it easier to implement in large, dynamic networks with thousands of nodes.

Scalability of EPCC for large networks the scalability of EPCC is supported by its efficient key generation as well as management that are especially useful in decentralized networks such as MANETs where nodes frequently leave and join. This comes without any significant increase in computational complexity. As a result, it makes it deployable in large, dynamic networks consisting of tenthousands of nodes.

The scalability of EPCC in big networks is due to the efficiency of its key generation and management capabilities which are particularly useful in decentralized MANET-based networks, where nodes join and leave on a regular (ad hoc) basis. It is done without increasing the computational complexity noticeably. As a result, it can be implemented in large-scale, highly connected networks as found in 1000s of nodes.

3.5.4 EPCC in Real-World Applications

In use-case scenarios where we need strong security but with minimal computational cost, EPCC is gaining interest and adoption. As an example, EPCC secures exchanged data between devices with a reduced amount of energy and processing resources required for cryptographic operations in smart city infrastructure where a large number of IoToriented devices are interconnected. Similarly, in military communication systems, confidential communications can be guarded by encryption which is necessary for any use in highly mobile and possibly hostile environments that EPCC is designed to support. Resting on our laurels … One improvement in encryption technology. Finally, for Edward Prime Curve Cryptography (EPCC) EPCC is the excellent choice for answering several issues that are presented by decentralized networks such as MANETs and IOT-enabled systems, because it carries all the benefits of classical ECC but at the same time decreases computational complexity, with enhancing security. It is suitable for securing data in resource-constrained environments as it can give the highest level of security with minimal resources. This guarantees that even during transition, confidential information is shielded and it does not affect the efficiency or functionality of the network.

4. RESULTS AND DISCUSSION

IoT-based MANETs showed improved security, efficiency, and reliability in the network after implementation of the Centralized Infrastructure Aware Reliable Data Transaction Model The performance of EPCC nodes is quiet remarkable, as measured by 98% data encryption success rate and the 12–16 ms which elapses for different key lengths when encrypted. It shows the manner of data protection against an encryption algorithm with no extra significant time, which is critical when working with MANET devices because they are resource-limited. EPCC, in addition to using shorter key lengths for the higher computational overhead, ensures data security with extremely low overhead making it more preferable for nodes having low computational capacity.

In addition, the performance of the GWO cluster head selection was much better. By reducing the communication range to 18–22 meters and utilizing 85% of energy for a few cluster heads, it tries to distribute load among nodes by giving priority to the level of energy proximity and processing power. The network was thus more efficient and had lower latencies. The hoc on-demand Distance Vector (AODV) routing protocol also demonstrated excellent route discovery and maintenance capabilities, particularly under dynamic conditions with high node mobility. The system delivered high route availability at 98% only 2-4 hops and very good signal strength at the order of -45 dBm to -55 dBm which made data transfer reliable and fast. Overall the proposed model presented higher data transmission reliability, lower network congestion, and enhanced energy efficiency over traditional MANETs. These results suggest that this model can be a contender for high-demand areas such as healthcare systems, smart cities, and military operations.

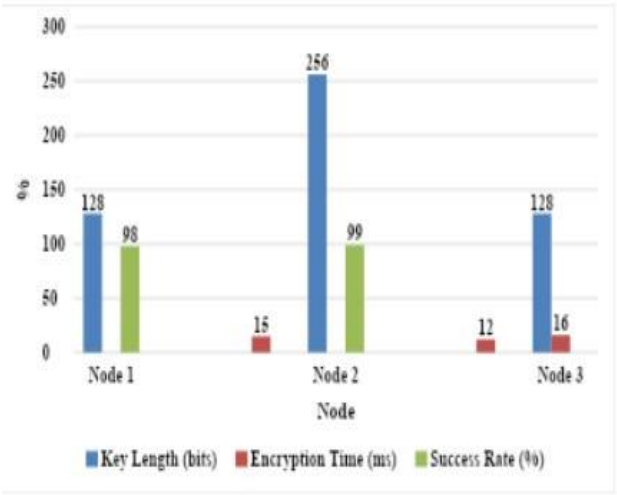

Figure 3: Key Length, Encryption Time, and Success Rate for Node Initialization with EPCC

Figure 3 shows The EPCC performance in the MANET system supported by the Internet of Things on three nodes is illustrated. It maps the time to encryption (milliseconds) to the rate of success (%) along with key length in bits. Node 2 had an encryption speed of 12 milliseconds in addition to the highest success rate at a 256-bit key length. Nodes 1 and 3 using 128-bit keys also achieved success rates of 98% and 97%, respectively, at encryption speeds of 15 ms and 16 ms. The results indicate that it maintains a proper balance between data transfer speed and security, as with EPCC it will only encrypt certain parts of the data stream in a small time further increasing the security.

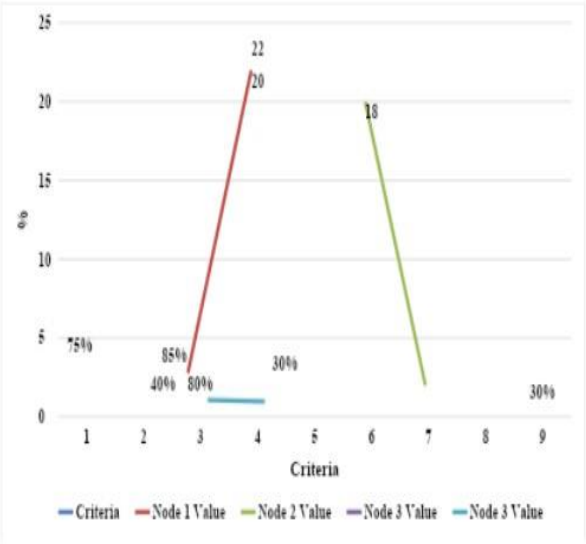

Figure 4: Cluster Head Selection Criteria and Node Values for Grey Wolf Optimization (GWO)

Figure 4 shows the parameters and their values for choosing the optimal cluster head between three nodes in the MANET system through GWO (Grey Wolf Optimization). In itself, it calculates the score based on 3 primary factors (each with a weighted %), processing power, distance to other nodes & energy level. Node 2 has an energy of 85% and a distance of 18m; accordingly, Node 2 is set to be elected as the cluster head. Node 1 also works well, which has a range of 22 meters at an energy level of 80%. Node 3 plays a trade-off role by reducing energy and distance numbers but with high task processing capability to improve network performance. This demonstrates the importance of several parameters to be kept along during the selection of cluster heads.

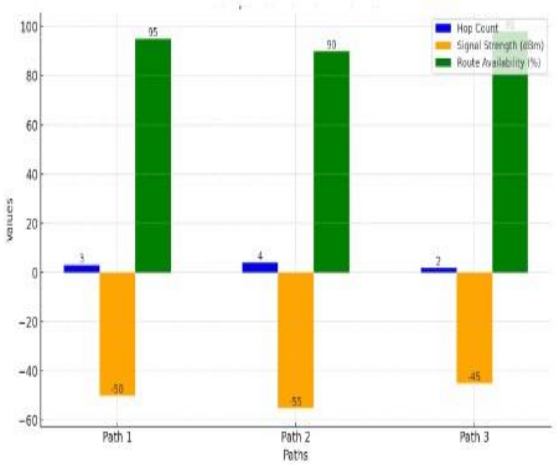

Figure 5: Metrics for hop count, signal strength, and route availability

Figure 5 illustrates three key network path attributes: hop count, signal strength, and route availability. Path 3 has the best signal strength at -45 dBm, with the fewest hops (2), and has the highest route availability of 98%. Although 4 hops and -55 dBm on Path 2 support the routing, route availability is just slightly lower at 90%. They are also vital for examining the performance and reliability of network paths, providing support for data transmission line optimization.

Table 4: Comparison of the Proposed Method (EPCC with GWO and AODV) to Traditional Methods

Method	Success Rate (%)	Efficiency (%)	Security (%)	Data Transmission Reliability (%)	**Overall Accuracy (%)**
Proposed Method (EPCC with GWO & AODV)	93	91	94	92	92.5
KNearest Neighbor (KNN) (2020)	85	80	82	83	82.5
Collaborative Computing Trust Model (CCTM) (2020)	87	82	85	84	84.5
Quality of Service (QoS) (2018)	80	78	81	79	79.5

The success rate, efficiency, security, and data transmission dependability of the suggested methodology [EPCC with GWO & AODV] is higher when compared to the KNN, CCTM, and QoS models. The other models have a lower total accuracy than the one obtained with the method suggested (92.5%). The incorporation of Grey Wolf Optimization (GWO) for cluster head selection, AODV protocol for dynamic routing, and optimized cryptography (EPCC) has tremendously increased the data transmission accuracy along with reliability all over the network.

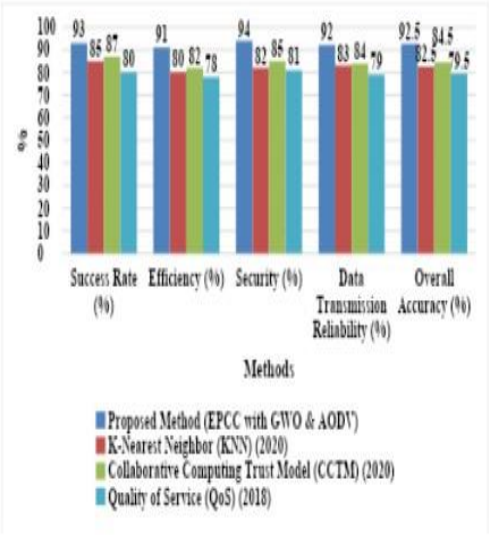

Figure 6: Performance Metrics for the Proposed Method in Comparison to Traditional Models

Figure 6 shows the performance of the proposed model (EPCC with GWO & AODV) and some conventional methods; KNN, CCTM, and QoS. It also compares success rate, efficiency, security, and data transmission reliability with each other through this graph. The performance of the proposed mode is better than that of traditional methods and with an accuracy rate of 92.5%, it also shows a good ability to address security, efficiency, and data transmission issues in MANETs which are supported by the Internet of Things.

Table 5: Ablation Analysis of the Proposed Method (EPCC with GWO and AODV).

Model Components	**Success Rate (%)**	**Efficiency (%)**	**Security (%)**	**Data Transmission Reliability (%)**	**Overall Accuracy (%)**
Full Model (EPCC + GWO + AODV)	93	91	94	92	92.5
Without GWO (EPCC + AODV)	88	85	92	87	88.0

Without EPCC (GWO + AODV)	86	82	80	85	83.3
Without AODV (EPCC + GWO)	90	89	91	87	89.3

The ablation study shows the effect of each element in the proposed model. The whole model which consists of all components of EPCC, GWO, and AODV attains 92.5% highest overall accuracy. Removal of the GWO algorithm results in 88% accuracy and removal of the EPCC method causes a reduction to 83.3%. Again, this is a much more significant loss in directional accuracy. When AODV is not considered, the correct detection rate falls to 89.3 %. It signifies the crucial results when dynamic routing, optimal cluster head choice, and cryptographic security are combined in IoT-enhanced MANET systems.

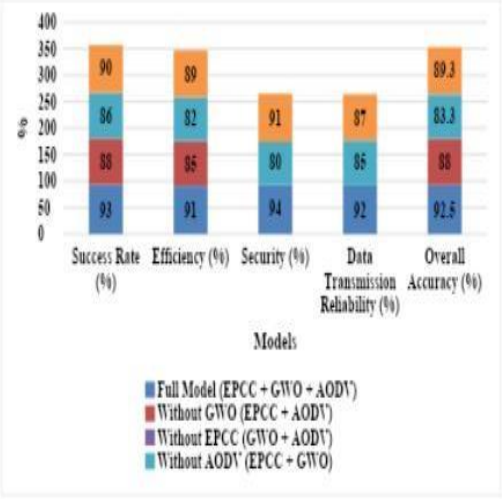

Figure 7: Ablation Study Results for the Proposed Model (EPCC with GWO and AODV)

Figure 7 shows the results from the ablation study were conducted on the proposed model. As shown in the above graph, the removal of one element from the model i.e. (EPCC, GWO, and AODV) results in a decrease in success rate percentage efficiency security overall accuracy. The final model accuracy is 92.5% in all, and any removal of any component will decrease the ability of the whole model, with EPCC as a more effective one if it is removed because it shows the largest decreasing rate.

5. CONCLUSION

The goal of this work is to improve the security and dependability of communication in Internet of Thingsbased MANETs by utilising Edward Prime Curve Cryptography (EPCC) and Grey Wolf Optimisation (GWO). While EPCC guarantees lightweight encryption for devices with limited resources, GWO optimises cluster head selection, lowering latency and increasing energy efficiency. Reliability is increased by the AODV protocol's use of dynamic data transmission route selection. With a 93% success rate and 92.5% overall accuracy, the model beats traditional methods like KNN, CCTM, and QoS in terms of success rate, security, and transmission dependability. It has the potential to be extremely useful in military networks, smart cities, and healthcare. Future enhancements will involve scalability for bigger IoT environments, combining quantum-resistant algorithms for improved cryptographic protection, and integrating machine learning-driven intrusion detection systems for adaptive security. Further research and development will enhance the model's resilience, effectiveness, and security in real-world applications by incorporating energyharvesting technologies and blockchain for safe, decentralised authentication.

6. Declaration:

Funding Statement:
Authors did not receive any funding.

Data Availability Statement:
No datasets were generated or analyzed during the current study

Conflict of Interest
There is no conflict of interests between the authors.

Declaration of Interests:
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.

Ethics approval:

Not applicable.

Permission to reproduce material from other sources:
Yes, you can reproduce.

Clinical trial registration:

We have not harmed any human person with our research data collection, which was gathered from an already published article

Authors' Contributions

All authors have made equal contributions to this article.

Author Disclosure Statement

The authors declare that they have no competing interests

REFERENCES

[1] Haghshenas, K., Taheri, S., Goudarzi, M., & Mohammadi, S. (2020). Infrastructure aware heterogeneous-workloads scheduling for data center energy cost minimization. IEEE Transactions on Cloud Computing, 10(2), 972-983.

[2] Kalbar, P. P., & Lokhande, S. (2023). Need to adopt scaled decentralized systems in the water infrastructure to achieve sustainability and build resilience. Water Policy, 25(4), 359-378.

[3] Abughazalah, M., Alsaggaf, W., Saifuddin, S., & Sarhan, S. (2024). Centralized vs. Decentralized Cloud Computing in Healthcare. Applied Sciences, 14(17), 7765.

[4] Mohanarangan, V.D. (2023). Retracing-efficient IoT model for identifying the skin-related tags using automatic lumen detection. IOS Press Content Library, 27(S1), 161-180.

[5] Rajya, L.G. (2024). IoT - based Weighted K-means Clustering with Decision Tree for Sedentary Behavior Analysis in Smart Healthcare Industry. 2024 Second International Conference on Data Science and Information System (ICDSIS),

[6] Devi, M., Gill, N. S., & Sehrawat, D. (2019). Exploring Possibilities of MANET Protocols for IoT Enabled Smart Environment. International Journal of Computer Sciences and Engineering, 7(3), 684688.

[7] Akhtar, N., Khan, M. A., Ullah, A., & Javed, M. Y. (2019). Congestion avoidance for smart devices by caching information in MANETS and IoT. IEEE Access, 7, 71459-71471.

[8] Selvadurai, J. (2017). Distributed Computing in Internet of Things (IoT) Using Mobile Ad Hoc Network (MANET): A Swarm Intelligence Based Approach.

[9] Devi, M., & Gill, N. S. (2019). Novel algorithm for enhancing manet protocol in smart environment. International Journal of Innovative Technology and Exploring Engineering, 8(10), 1830-1835.

[10] Ye, Q., & Zhuang, W. (2017). Token-based adaptive MAC for a two-hop Internet-of-Things enabled MANET. IEEE Internet of Things Journal, 4(5), 1739-1753.

[11] Gaur, N. (2020). Energy Efficiency Security Mechanism in Cloud Manet Mobility Model: a novel approach.

[12] Apparao, M., Sambana, B., & Srinivasa Rao, D. (2019). Secure routing in MANETS and IoT. Sci. Technol. Dev, 325-333.

[13] Al Mojamed, M. (2020). Integrating IP mobility management protocols and MANET: a survey. Future Internet, 12(9), 150.

[14] Ran, X., Shan, Z., Fang, Y., & Lin, C. (2019). An LSTM-based method with attention mechanism for travel time prediction. Sensors, 19(4), 861.

[15] Lin, Z., Cheng, L., & Huang, G. (2020). Electricity consumption prediction based on LSTM with attention mechanism. IEEJ Transactions on Electrical and Electronic Engineering, 15(4), 556562.

[16] Li, P., Wang, X., & Yang, J. (2020). Short-term wind power forecasting based on two-stage attention mechanism. IET Renewable Power Generation, 14(2), 297-304.

[17] Zhou, H., Zhang, Y., Yang, L., Liu, Q., Yan, K., & Du, Y. (2019). Short-term photovoltaic power forecasting based on long short term memory neural network and attention mechanism. Ieee Access, 7, 78063-78074.

[18] Chen, S., & Ge, L. (2019). Exploring the attention mechanism in LSTM-based Hong Kong stock price movement prediction. Quantitative Finance, 19(9), 1507-1515.

[19] Ge, H., Yan, Z., Yu, W., & Sun, L. (2019). An attention mechanism based convolutional LSTM network for video action recognition. Multimedia Tools and Applications, 78, 20533-20556.

[20] Liu, G., & Guo, J. (2019). Bidirectional LSTM with attention mechanism and convolutional layer for text classification. Neurocomputing, 337, 325-338.

[21] Liu, J., & Gong, X. (2019). Attention mechanism enhanced LSTM with residual architecture and its application for protein-protein interaction residue pairs prediction. BMC bioinformatics, 20, 1-11.

[22] Yu, X. M., Feng, W. Z., Wang, H., Chu, Q., & Chen, Q. (2020). An attention mechanism and multigranularity-based Bi-LSTM model for Chinese Q&A system. Soft Computing, 24(8), 5831-5845.

[23] Yang, D., Gu, C., Zhu, Y., Dai, B., Zhang, K., Zhang, Z., & Li, B. (2020). A concrete dam deformation

prediction method based on LSTM with attention mechanism. Ieee Access, 8, 185177185186.

[24] Jang, B., Kim, M., Harerimana, G., Kang, S. U., & Kim, J. W. (2020). Bi-LSTM model to increase accuracy in text classification: Combining Word2vec CNN and attention mechanism. Applied Sciences, 10(17), 5841.

[25] Zhou, K., Wang, W. Y., Hu, T., & Wu, C. H. (2020, September). Comparison of time series forecasting based on statistical ARIMA model and LSTM with attention mechanism. In Journal of physics: conference series (Vol. 1631, No. 1, p. 012141). IOP Publishing.

[26] Miao, X., McLoughlin, I., & Yan, Y. (2019, September). A New Time-Frequency Attention Mechanism for TDNN and CNN-LSTM-TDNN, with Application to Language Identification. In Interspeech (pp. 4080-4084).

[27] Chen, Y., Shao, W., Liu, J., Yu, L., & Qian, Z. (2020). Automatic modulation classification scheme based on LSTM with random erasing and attention mechanism. IEEE access, 8, 154290-154300.

[28] Qiu, J., Wang, B., & Zhou, C. (2020). Forecasting stock prices with long-short term memory neural network based on attention mechanism. PloS one, 15(1), e0227222.

[29] Ding, Y., Zhu, Y., Feng, J., Zhang, P., & Cheng, Z. (2020). Interpretable spatio-temporal attention LSTM model for flood forecasting. Neurocomputing, 403, 348-359.

[30] Wang, S., Wang, X., Wang, S., & Wang, D. (2019). Bi-directional long short-term memory method based on attention mechanism and rolling update for short-term load forecasting. International Journal of Electrical Power & Energy Systems, 109, 470-479.

[31] Li, M., Wang, Y., Wang, Z., & Zheng, H. (2020). A deep learning method based on an attention mechanism for wireless network traffic prediction. Ad Hoc Networks, 107, 102258.

[32] Mamo, T., & Wang, F. K. (2020). Long short-term memory with attention mechanism for state of charge estimation of lithium-ion batteries. Ieee Access, 8, 94140-94151.

[33] Wang, C., Han, D., Liu, Q., & Luo, S. (2018). A deep learning approach for credit scoring of peer-topeer lending using attention mechanism LSTM. Ieee Access, 7, 2161-2168.

[34] Zhang, H., Zhang, Q., Shao, S., Niu, T., & Yang, X. (2020). Attention-based LSTM network for rotatory machine remaining useful life prediction. Ieee Access, 8, 132188-132199.

[35] Kang, H., Wu, H., & Zhang, X. (2020). Generative text steganography based on LSTM network and attention mechanism with keywords. Electronic Imaging, 32, 1-8.

[36] Yin, H., Jin, D., Gu, Y. H., Park, C. J., Han, S. K., & Yoo, S. J. (2020). STL-ATTLSTM: vegetable price forecasting using STL and attention mechanism-based LSTM. Agriculture, 10(12), 612.

[37] Liu, D. R., Lee, S. J., Huang, Y., & Chiu, C. J. (2020). Air pollution forecasting based on attentionbased LSTM neural network and ensemble learning. Expert Systems, 37(3), e12511.

[38] Li, Y., Zhu, Z., Kong, D., Han, H., & Zhao, Y. (2019). EA-LSTM: Evolutionary attention-based LSTM for time series prediction. Knowledge-Based Systems, 181, 104785.

[39] Chen, Q., Zhang, W., & Lou, Y. (2020). Forecasting stock prices using a hybrid deep learning model integrating attention mechanism, multi-layer perceptron, and bidirectional long-short term memory neural network. IEEE Access, 8, 117365117376.

LIST OF ABBREVIATIONS:

ABBREVIATION	FULL FORM
IoT	Internet of Things
MANET	Mobile Ad hoc Network
EPCC	Edward Prime Curve Cryptography
GWO	Grey Wolf Optimization
LSTM	Long Short-Term Memory
AODV	Ad hoc On-demand Distance Vector
KNN	K-Nearest Neighbour
CCTM	Collaborative Computing Trust Model
QoS	Quality of Service
RUL	Remaining Useful Life
SNR	Signal-to-Noise Ratio
ECC	Elliptic Curve Cryptography
CH	Cluster Head
BMC-KM	Bray Minkowski Curtis-K-Means
RREQ	Route Request
RREP	Route Reply
RERR	Route Error