An Intelligent Buffalo-Based Secure Edge-Enabled Computing Platform for Heterogeneous IoT Network in Smart Cities

REYAZUR RASHID IRSHAD [1], SHAHID HUSSAIN [2] IHTISHAM HUSSAIN [3], IBRAR AHMAD[4], ADIL YOUSIF [1], IBRAHIM M. ALWAYLE [1], AHMED ABDU ALATTAB [1], KHALED M. ALALAYAH [1], JOHN G. BRESLIN [5], MOHAMMED MEHDI BADR [1], AND JOEL J. P. C. RODRIGUES [6].

[1]Department of Computer Science, College of Science and Arts, Sharurah-68341, Najran University, Kingdom of Saudi Arabia (email: rrirshad@nu.edu.sa, ayaffaki@nu.edu.sa, alwayle1@yahoo.com, aaalattab@nu.edu.sa, kmalalayah@nu.edu.sa, mohfbadr2000@yahoo.com)

[2]Inovative Value Institute (IVI), School of Business, National University of Ireland Maynooth (NUIM), Maynooth, W23 F2H6, Ireland (email: shahid.hussain@mu.ie)

[3]Department of Computer Science, Abdul Wali Khan University (AWKU), Pabbi Campus (email: ihtishamhussain922@gmail.com)

[4]Department of Computer Science University of Shangla Pakistan (email: ibrar2545@gmail.com)

[5]Department of Electrical and Electronic Engineering, Data Science Institute, University of Galway, H91 TK33 Galway, Ireland (email: john.breslin@universityofgalway.ie)

[6]COPELABS, Lusófona University, Campo Grande 376, 1749-024 Lisbon, Portugal (email: joeljr@ieee.org)

Corresponding authors: John G. Breslin and Shahid Hussain (e-mail: john.breslin@universityofgalway.ie and shahid.hussain@mu.ie).

The authors are thankful to the Deanship of Scientific Research at Najran University for funding this work, under the General Research Funding program grant code (NU/DRP/SERC/12/11).

ABSTRACT The Internet of Things (IoT) based Smart city applications are the latest technology-driven solutions designed to collect and analyze data to enhance the quality of life for urban residents by creating more sustainable, efficient, and connected communities. Communication nodes are networked independently to monitor the circumstances, where they require being more energy-efficient and securing, to improve the performance of sustainable cities. Because, the enormous number of networked devices makes the smart cities application vulnerable to many security breaches, all of which have serious ramifications for a city and its residents' safety, well-being, and economic development. Low-powered sensors have limitations in terms of battery life, short transmission range, and security considerations, despite the fact that the combination of edge computing and Green IoT considerably enhances network performance in terms of processing and data storage. Consequently, it is necessary to implement an advanced approach to provide energy resources with secure data transmission for sustainable cities. Therefore, this research proposes an Intelligent Buffalo-based Secure Edge-enabled Computing (IB-SEC) framework for smart cities by IoT platform, which aims to enhance communication efficiency, and reliability, with minimizing latency in terms of energy consumption and data security for data transmission. The developed IB-SEC platform utilizes a combination of the African Buffalo Optimization (ABO) algorithm and a Distributed Hash function-based security algorithm to enhance the efficiency, security, and reliability of data transmission in IoT-based smart city networks. This platform leverages the capabilities of secure edge computing and MAC protocols to achieve its goals, by implementing encryption, authentication, and access control mechanisms that ensure the wireless communication is secure, and the data is protected against unauthorized access. Overall, the IB-SEC framework provides an advanced approach to secure IoT networks and enable smart city applications. Moreover, the developed platform enables the integration of heterogeneous edge devices, sensors, and systems which is effectively managed and adapted by Median Access Control (MAC) protocols. The IB-SEC is implemented in MATLAB and validated through cutting-edge security algorithms in terms of improved security, reliability, throughput, and reduced latency and energy consumption.

INDEX TERMS African buffalo Algorithm, Internet of Things, smart city, heterogeneous, Secure Edge enabled computing.

I. INTRODUCTION

SMART cities are metropolitan regions that employ data-driven technology to improve their efficiency, sustainability, and quality of life for their residents [1]. The concept of smart cities has gained significant traction in recent years due to the advancement of the Internet of Things (IoT), big data, and artificial intelligence (AI) technologies [2]. These technologies enable cities to collect and analyze data from various sources, including sensors, mobile devices, and social media, to improve their operations and services. Smart cities offer a range of benefits, including energy efficiency, improved traffic flow, reduced crime rates, and enhanced citizen engagement [3]. Nowadays, communication and information technologies are being developed with the aim of creating smart city-based applications [4]. These technologies are built on advanced computer knowledge and are designed to support social networking fields, cloud computing, and the IoT within smart cities. In the context of smart cities, the broadband network plays a critical role as it utilizes advanced communication protocols such as MAC [5]. Wireless technologies are also important in enabling smooth technical evolution and offering personalized services within smart cities. Besides, the IoT serves as the foundational building block for creating a digitalized representation of a smart city environment [6]. Consequently, by interconnecting smart objects using heterogeneous communication modes, smart cities are able to exploit resources directly, providing ubiquitous and reliable services that enable easy access to information [7, 8]. The system boasts a large volume of data interconnecting capability, allowing a wide range of devices such as sensor devices, electronic devices, vehicles, and machines to connect seamlessly to the smart city environment without any loss of communication [9, 10]. This feature is critical for ensuring the effective operation of smart city applications and services that rely on real-time data exchange and analysis. By facilitating high-speed and reliable data transmission, this prototype can support the smooth functioning of various smart city operations, such as traffic management, energy usage optimization, and environmental monitoring. In order to provide reliable services to users, smart city applications are often directly supported by various technologies that facilitate the sharing and exchange of data across different smart city environments and applications, various technologies are being used [11, 12]. Information and Communication Technologies (ICT) have enabled the deployment of a wide range of public and private Mobile Edge Computing (MEC) modules, which can effectively provide seamless access in a smart environment. However, ensuring security is an important aspect of performance in a smart city environment, particularly with the interconnecting technologies and open communication [13]. The deployment of smart city applications and interoperable technologies, which are enabled by ICT, has made it possible to provide security protection towards the heterogeneous IoT structure via adapting of security measures within the ICT module that ensure both public and private data integrity through authenticated resources, enabling the design of effective security measures for smart city applications and services [14, 15, 16]. The innovation of heterogeneous IoT sensors is enabled by remote communication technologies, which allows for the monitoring and control of IoT nodes within the verification area and enables the processing and monitoring of data in real-time, providing valuable insights for various smart city applications and services [17]. In addition to ensuring functional tracing of objects, IoT nodes also play an important role in maintaining the performance of smart city applications [18]. The selection of the MAC protocol has a significant impact on the energy consumption of IoT nodes and thus can be classified into three types: hybrid, contention-based, and contention-free protocols [19]. To mitigate undirected channel access with correspondent carrier frequency, Time Division Multiple Access (TDMA) mechanisms are often adapted within contention-free MAC protocols [20]. Despite its advantages, TDMA has some drawbacks, such as variable network load, inefficient channel detection, and limited network scalability [21]. When selecting a MAC protocol for IoT devices in a smart city environment, it is important to carefully consider the advantages and drawbacks of various options, such as TDMA, contention-based MAC protocols, and hybrid MAC protocols that can be affected by large-density networks and energy depletion [22, 23]. Various techniques have been developed to address the drawbacks of IoT-based smart city applications, including resource restrictions and protocol security, such as edge-enabled reliable data transmission protocols that aim to prevent attacks and improve network lifetime [24]. A clustering-based particle swarm optimization model has been developed to mitigate security threats during data transmission [25]. With the increasing number of security threats in the smart city environment, new strategies are being introduced to protect information from malware actions. One such strategy is the use of unsupervised machine learning, which can help to detect and prevent potential attacks by analyzing large amounts of data and identifying patterns and anomalies in real-time [26, 27]. Also, a three-phase deployment approach has been proposed to determine the probability function of edge servers, but it fails to accurately address several issues. Thus, there exists a knowledge gap in MAC protocols for IoT-based smart city applications related to the efficient selection and adaptation of MAC protocols to the diverse requirements of smart city devices, including varying traffic loads, energy consumption, and security needs, while addressing the limitations of existing protocols [28]. Consequently, the proposed IB-SEC platform aims to fill the knowledge gap by integrating secure edge computing and MAC protocols to enhance the efficiency, security, and reliability of IoT networks in smart cities, addressing the diverse requirements of smart city devices, and repelling hacker attempt through secure data transmission. The key contribution of this paper is summarized in three folds.

- We have developed the Intelligent Buffalo-based Secure

Edge-enabled Computing (IB-SEC) platform, which is designed based on secure edge computing and MAC protocols to enhance the efficiency, security, and reliability of IoT networks in smart cities. The IB-SEC is the combination of African Buffalo Optimization (ABO) with Distributed Hash function-based security algorithm. The developed platform leverages the power of secure edge computing and MAC protocols to enhance the efficiency, security, and reliability of IoT networks in smart cities. This is achieved through a combination of encryption, authentication, and access control mechanisms that secure wireless communication and protect the data from unauthorized access.

- The proposed IB-SEC analyzes data in real-time, enabling it to detect and respond to potential security threats quickly by monitoring and processing the IoT networked data flows, and incorporates a range of security mechanisms, including encryption, authentication, and access control, to ensure that data is protected at all times. Moreover, by processing data locally at the edge of the network, IB-SEC can reduce the time it takes to transmit data to and from central data centers, resulting in faster response times and improved overall performance.
- The execution of this research is carried out using MATLAB programming. It identifies the scalability needs and conducts a comparative analysis of the current state-of-the-art IoT platforms based on several criteria. The performance of the proposed approach is validated with different measures such as throughput, energy consumption, security, latency, and reliability.

The organization of this paper is provided as follows: Section II briefly reviews the literature of previous implementations in the field of IoT-enabled smart cities and associated challenges. The problem statement is detailed in Section III. Section IV describes the proposed methodology. Section V discusses the results and the efficiency of the proposed model compared to traditional models. Finally, Section VI concludes the paper.

II. LITERATURE SURVEY

Internet-of-Things-based smart city technologies enhance the quality of life and provide promising solutions for multiple functions, such as resource utilization, healthcare monitoring, and resource management systems that gather data from various sensor devices. However, the collected information is highly vulnerable to attacks from end-users, which poses a significant security threat to the smart city application [29].

Altar, Ayesha, et al. [28] presented a context-based trust model to mitigate service-oriented attacks in smart cities operating in IoT networks. Their proposed model considers various contextual factors, such as device type, user behavior, and environmental conditions, to assess the trustworthiness of entities involved in service interactions. The model also employs a reputation-based approach to enhance the accuracy of trust evaluation. The authors evaluated the proposed model using a smart city scenario and demonstrated its effectiveness in detecting and mitigating service-oriented attacks. The results show that the proposed model achieved high accuracy in detecting attacks while maintaining a low false positive rate, thus providing a reliable and efficient solution for securing smart cities in IoT networks. However, one limitation of this paper is that the proposed context-based trust model may have high computational overhead due to the need for processing large amounts of contextual data. Nevertheless, the authors evaluated the proposed model using a single smart city scenario, and the effectiveness of the model in different smart city environments and under different attack scenarios has yet to be investigated.

Mehdi Gheisari et al. [30] proposed an ontology-based privacy-preserving (OBPP) framework for IoT-based smart cities. The framework enables the creation of a privacy ontology that can be used to define privacy policies and privacy-related concepts in a smart city context. The authors implemented the OBPP framework and evaluated it using a case study of a smart transportation system. The results showed that the framework effectively enhanced the privacy protection of IoT-based smart city applications while minimizing the impact on system performance. Nonetheless, the OBPP framework does not address the issue of user consent and how it can be incorporated into the privacy ontology.

Abd El-Latif, Ahmed A, et al [31] proposed a quantum-inspired blockchain-based approach to cybersecurity for securing smart edge utilities in IoT-based smart cities. The approach utilizes quantum computing principles to enhance blockchain security and protect against attacks, and it was evaluated using a smart grid system. The authors demonstrated the effectiveness of the proposed approach in detecting and mitigating cyber-attacks, highlighting the potential of quantum-inspired blockchain-based cybersecurity as a secure and efficient solution for IoT-based smart cities. However, their proposed approach has a high computational overhead due to the use of quantum-inspired computing principles; besides, the approach also limits the generalization of IoT-based smart city applications.

Mohammed Mikail Salim et., al. [32] proposed a method for securing smart cities against botnet attacks using the Long Short-Term Memory (LSTM) algorithm and lightweight containers. The authors highlight the vulnerability of smart cities to cyberattacks and the potential harm that such attacks can cause. They introduce a container-based approach to isolate the application, and they use the LSTM algorithm to analyze the network traffic and identify botnet attacks. The proposed method is evaluated using a dataset of botnet attacks and compared with other state-of-the-art methods. The results show that the proposed method is effective in detecting and mitigating botnet attacks and outperforms other methods in terms of accuracy and efficiency. The paper concludes that the proposed method can be applied to secure smart cities against botnet attacks and enhance their security. The paper's evaluation is limited to a single dataset of botnet attacks, which may not reflect the variety of attack scenarios that

could be encountered in a real-world smart city environment, and the potential resource requirements of implementing the proposed method are not discussed.

Salim, Mikail Mohammed, et al. [33] presented a method for detecting attacks in IoT-based smart cities using an intrusion detection system (IDS) based on a modified adaptive neuro-fuzzy inference system (MANFIS) classifier and securing data transmission using the improved RSA (IRSA) encryption technique. The proposed method is evaluated using a smart city dataset and compared with other state-of-the-art methods, demonstrating its effectiveness in detecting attacks and ensuring secure communication in a smart city environment. The paper concludes that the proposed method can be applied to enhance the security and privacy of smart cities. Nevertheless, the paper did not compare the proposed method with existing state-of-the-art methods and did not discuss the feasibility and scalability of implementing the system in real-world smart city environments.

The current knowledge gap in IoT-based smart cities regarding MAC protocols, communication networks, and security highlights the need for more research to develop integrated solutions that can address the challenges of congestion, interference, and security threats while ensuring efficient and reliable communication between a massive number of IoT devices. This includes the selection of secure and efficient MAC protocols that enables security mechanisms, support seamless communication, and protect IoT devices from cyberattacks and privacy breaches in the smart cities environment. This paper proposes a platform called IB-SEC that combines secure edge computing and MAC protocols to improve the efficiency, security, and reliability of IoT networks in smart cities. A key research worry for a dynamic and large-sized IoT-incorporated next-generation sensor system has been identified based on the previously mentioned prior work: effective use of energy with dependable and scalable routing. Similar evidence has shown that the majority of current solutions are unable to modify routing performance in accordance with the dynamic communication model. According to the above-mentioned problem, intelligent optimization with a secured distributed hash function is proposed for IoT-based smart city applications.

III. PROBLEM STATEMENT

Security and privacy are significant challenges associated with IoT-based smart city applications that gather and analyze a vast amount of data on a common IoT platform, which makes it susceptible to numerous attacks [21]. In IoT-based smart city applications, security is a critical concern since the data collected is sensitive and can include personal information such as location, behavior, and habits. Any data breach can result in severe consequences for individuals and the entire city. Moreover, as IoT-based smart city applications become more prevalent, the potential for cyber-attacks increases. Attackers can exploit vulnerabilities in the system to gain unauthorized access, steal data, or manipulate the system, resulting in significant economic and social consequences. Privacy is another significant challenge in IoT-based smart city applications. These systems collect and analyze data from various sources, including sensors, cameras, and other devices, which can lead to the invasion of individuals' privacy. Individuals may not be aware of the data collected or how it is used, leading to concerns about their fundamental rights. Therefore, proper security and privacy measures must be put in place to protect the data collected and maintain the trust of the citizens. However, IoT-enabled smart cities have implemented multi-layered response mechanisms to quickly activate emergency protocols [34]. Reliability issues have become increasingly prevalent in IoT communication. Several challenges related to reliability can result in failures of smart devices [35]. Additionally, malicious nodes have the ability to mishandle network data and compromise the privacy of sensor data. Furthermore, malicious nodes can mishandle network data and compromise the privacy of sensor data. This issue is particularly critical in real-time applications such as agriculture, military, healthcare, and other sensitive fields. Additionally, IoT sensor devices process vast amounts of information transmitted over an unsecured internet [36, 37, 38]. As a result, ensuring authentication, privacy, and data integrity are crucial research challenges for IoT applications. The problem statement is provided in Algorithm 1.

Algorithm 1 The Security Importance of IoT Network

Inputs : Node density and their initial energy
Outputs: Secure data with dropping malicious packet
Transmission
Compute latency based on starting and ending time.
$l_i, j = (1 - n_i) * l_i, t + n_i * edgel_i, t$
Compute Consumed Energy.
$E_i, j = (1 - n_i) * E_i, t + n_i * totalE_i, t$
Limit is supposed to be met
$l_i, j \leqq lt_i and E_i, j \leqq E_m ax$
The objective issue is
$x_i, j = \alpha * \frac{l_i, j}{l_m ax} + (1 - \alpha) * \frac{E_i}{E_m ax}$
Security
Find the malicious data attack
Drop the malicious data packet

IV. THE PROPOSED INTELLIGENT BUFFALO-BASED SECURE EDGE-ENABLED COMPUTING PLATFORM

The IoT in smart cities has gained significant attention as a communication system due to the ability of numerous wireless systems to connect over the internet. Smart cities include various applications like public safety, environmental monitoring, traffic management, smart transportation, energy management, and so on. However, the security threats associated with IoT can have far-reaching consequences, making it an important issue for IoT-enabled smart cities. The vast amounts of data generated and transmitted by IoT devices can be compromised, resulting in data breaches, privacy violations, and even physical harm. As more and more devices become connected to the internet, they become potential targets for cyber-attacks.

A practical example of the security threats in IoT-enabled smart cities could be a cyber-attack on the traffic management system. Suppose the traffic management system is integrated with various IoT devices such as sensors, cameras, and automated traffic signals, and it is connected to the cloud infrastructure. In that case, a cyber-attack on the system could compromise the entire transportation network, leading to severe traffic congestion, accidents, and even loss of life. The attackers could potentially gain access to the traffic management system by exploiting vulnerabilities in the cloud infrastructure or by compromising the IoT devices connected to the system. Once the attackers gain access, they could manipulate the traffic signals, disrupt the sensors, and even manipulate the data transmitted to the cloud, causing chaos in the transportation network. This scenario highlights the practical implications of security threats in IoT-enabled smart cities and emphasizes the need for robust security measures in the cloud infrastructure that supports these systems. Implementing security measures such as access controls, encryption, and intrusion detection systems can help mitigate the risk of cyber-attacks and protect the safety and privacy of citizens.

The IBSEC can help solve the security problems highlighted in the traffic management system scenario by providing a secure computing platform at the edge of the network and thus integrates multiple layers of security, such as access control, authentication, and encryption, to secure the traffic management system's data and devices. Moreover, the proposed platform uses machine learning algorithms to ana-lyze traffic patterns, detect anomalies, and identify potential security threats, while reducing the latency and improving the system's responsiveness by processing the data at the edge of the network. In the case of a cyber attack on the traffic management system, IBSEC can detect the intrusion, isolate the affected devices, and prevent the attack from spreading to other parts of the network, and can enable real-time alerts to the system administrators, enabling them to take immediate action and mitigate the potential impact of the attack. Therefore, ensuring the security of IoT systems is critical for protecting sensitive data and infrastructure in smart cities [39]. To address this issue, the proposed IB-SEC module is introduced which is based on secure edge computing technology and is designed to be energy-efficient and suitable for battery-powered devices, as presented in Fig. 1. The proposed module provides a means to enhance the security of IoT devices in smart cities by enabling secure edge computing and offers several advantages, such as it provides a secure computing environment for IoT devices at the edge of the network. This means that the data generated by these devices is processed and analyzed locally, reducing the need to send data to the cloud for analysis. This reduces the risk of data breaches and ensures the privacy of the data generated by IoT devices. Moreover, the proposed IB-SEC module plays a critical role in managing energy usage of battery-powered IoT devices in smart cities by optimizing energy consumption and extending the battery life of devices. According to the observation, the proposed IB-SEC Platform consists of innovative hardware and software technologies, together with edge computing and security capabilities. For a variety of use cases, from industrial automation to smart cities, the suggested architecture is an excellent platform because of these factors. The IoT devices are monitoring the environment and collecting their data for the different applications, the data is processed and transmitted to their corresponding decision-making systems. The developed IB-SEC Platform utilizes the computing architecture that utilizes edge computing and security technologies to provide enhanced performance and security for data processing and storage. The role of the Intelligent Buffalo-Based Secure Edge is to provide a secure, distributed computing environment that allows for the efficient processing of data at the edge of the network, without the need to transmit data back to a centralized server for processing. This architecture provides several benefits, including reduced latency, improved performance, and enhanced security by minimizing data exposure to the outside network. It utilizes the ABO which is a metaheuristic optimization algorithm inspired by the herding behavior of African buffalo. It computes the fitness function to evaluate each candidate IoT device based on the (i.e., security, energy efficiency, connectivity, processing power, and cost) criteria and assigns a fitness value accordingly. Initially, the energy of each node and node density is computed from the applications. For each sensor node finds its sub-path for data transmission. The ABO algorithm can then be used to optimize the selection of the finest route based on the fitness values of the candidate IoT device. The node with the highest fitness value would be selected as the finest route to transmit data with high security in the IoT-enabled smart city application. Consequently, Distributed Hash Table (DHT) for key-based data routing is applied for security improvements. The MAC layer is further used which is in charge of coordinating access between IoT gadgets in the common wireless medium, it is essential to develop an effective MAC protocol in an IoT system if high throughput and energy efficiency are to be achieved. Here, the MAC address verification is applied for effective data transmission. Additionally, MAC protocols help to minimize data collisions and improve overall network performance, which is essential for the efficient processing of data at the edge of the network.

A. PROCESS OF PROPOSED IB-SEC METHODOLOGY

The IoT devices enabled in smart cities have facilitated the development of several real-time applications to monitor environmental information, making cities smarter and more sustainable. Moreover, IoT sensor devices have enabled network users to configure various settings from the source or base station to the destination, using the internet. Consequently, IoT devices are installed in smart cities with efficient detection fields for identifying activities within specific boundaries. These IoT sensor devices can be sent to edge servers for analysis and processing, thus improving performance. Furthermore, edge servers are powerful enough

to handle heavy computations. The first step in this process is to calculate the energy consumption of each transmitting node, which is denoted by Eq. (1).

$$E'_T = \begin{cases} s'(E' + E'_b \times d'^2) & if d' \leq d'_t \\ s'(E' + E'_a \times d'^4) & if d' < d'_t \end{cases} \quad (1)$$

Where, E'_T represents the energy consumption of the transmitter node, s' and d' denote the size of the transmitted data bits and distance between source and destination respectively. Moreover, d' represents the transmission energy of each data bit, E'_b is a balanced energy level, d'^2 and d'^4 represent the transmission round. Consequently, the transmitted data bits are received at the destination sides. On the receiver side receiving node has dissipated the energy consumption $E'_r(s')$ as given in Eq. (2).

$$E'_r(s') = E' \times s' \quad (2)$$

The proposed IB-SEC module includes model setup, efficient data transmission, an optimization scheme, and security using a hash function. Initially, the IoT sensor nodes transmit data bits to recognize their neighbors for broadcasting data. Moreover, IoT devices are deployed in smart cities using a mesh topology, where all IoT nodes are adjacent to their shortest neighbors. Consequently, each IoT node saves data about its shortest neighbors and updates it in the MAC layer. Furthermore, to achieve effective and optimal results, the edge computing module uses an optimization algorithm to select a trusted node based on a fitness function. The ABO [40] algorithm is utilized here to perform optimal computations that generate appropriate activities. In addition, edge computing encompasses a large range of IoT devices that are equipped with edge servers to broadcast data bits through an uncontrolled and insecure wireless medium. This activity can pose network threats and compromise data safety, leading to negotiations on security. Hence, the proposed module provides enhanced security for IoT devices and ensures secure transmission from source to destination via the edge servers.

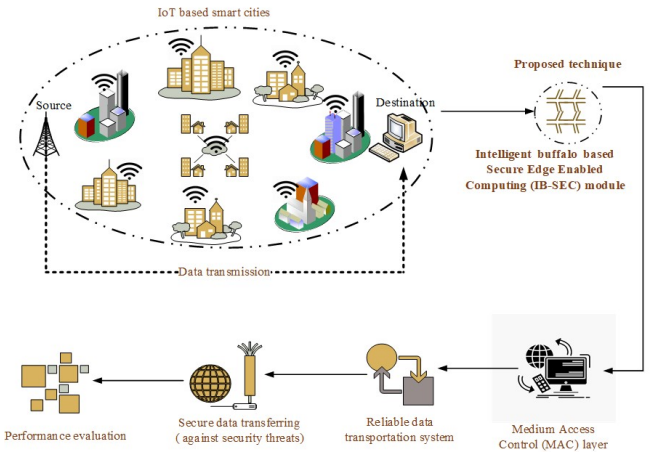

FIGURE 1. The architecture of proposed intelligent buffalo-based secure edge-enabled computing platform

1) Reliable data transportation system

The proposed model has adopted IoT nodes arranged in a mesh topology. This topology can reduce network disconnections, but may also result in incorrect data transmission paths. Initially, the step sets the initial parameters required for the program to function correctly. The IoT network is created with node A_{max} and its adjacent nodes $v^{'}$. The communication path $(C_{i,j})$ is defined between the nodes i and j. Edge servers initially create a partial mesh structure to coordinate each IoT node throughout the smart city. Then, the IoT nodes and data bits are updated in the population size of the ABO function. The fittest node is selected using an exploration and exploitation fitness function, as given in Eq. (3).

$$N_{t+1} = N_t + l_{a1}(A_{max} - Gf_t) + l_{a2}(A_{max.t} - Gf_t) \quad (3)$$

Where, N_{t+1} denotes a particular node selecting with the fitness function iteration limit is $(t-0, 1, 2, \cdots .)$, the learning parameters are expressed as l_{a1}, and l_{a2}, overall nodes are denoted as A_{max} and each node position is represented as $A_{max.t}$. If the exploration fitness function does not select the best node, then the algorithm switches to the exploitation fitness function using the following Eq. (4).

$$Gf_{t+1} = \frac{N_t + Gf_t}{\eta} \quad (4)$$

Where, η is assumed to be the random solution in the range of [0, 1]. Once the node is selected using the above function, the criteria are met and the algorithm stops. Otherwise, the iteration continues until the finest results are achieved.

2) Secure data transferring

This section details the performance of secure data transfer based on distributed hashing algorithms. Secret keys are created between the source and selected nodes to establish a symmetric key interchange arrangement [41, 42]. After that, data bits are forwarded to the edge server with the help of the selected nodes. Moreover, secret key generation is done using Eq. (5).

$$S'_k = P'_2(\alpha) mod x' = P'_1(\beta) mod x' \quad (5)$$

Where, S'_k is the secret key of both S'_i and S'_j nodes data transportation, $P'_2(\alpha) mod x'$ is the private key of α node and transfers node x'. Similarly, $P'_1(\beta) mod x'$ private key β of node and transfers node x'. Next, the distributed hash function is updated to improve the constraint level using Eq. (6).

$$H'_n = (D'_n \oplus S'_k) + R \quad (6)$$

Where, H'_n is an input function it will generate the digital hash function as H'_{n+1} with the help of the XoR gate. Then, the source node is incorporated with transmitted data and generates a secret key. Moreover, the digital hash function as H'_{n+1} is given in Eq. (7).

$$H'_{n+1} = (D'_n \oplus S'_k) + R_{n+1} \quad (7)$$

Based on equation (7) above, the overall network data-sharing process is achieved without sharing the secret key for security concerns.

The proposed IB-SEC module is demonstrated in Algorithm 1, which provides an algorithmic representation of the steps involved. The main steps are performed as follows:

Algorithm 2 IB-SEC Module

Inputs : Node density and their initial energy
Outputs: Secure data with dropping malicious packet
Initialization
  Initialize all parameters
Transmission
  for *each sensor node (Sn) in the network* **do**
    Find its sub-path
    Determine (x_1, x_2,x_3)
     $x_1 \leftarrow$ Node density$Extracted from IoTarch.$
     $x_2 \leftarrow$ Set initial energy$Node cost$
     $x_3 \leftarrow$ Response time$Based on edge server$
     if *(Route is not found in* x_1*)* **then**
      Unicast request
    end
    else
      Return *Null*
    end
  end
  Security
    Utilize a DHT for key-based data routing
     if *(the MAC address verification is true)* **then**
      $D' \leftarrow S'_k \oplus H'_n$
       Allow the data packet
    end
    else
      Drop the malicious data packet
    end
  Calculate the corresponding statistics
   Print the results

V. SIMULATION EXPERIMENTS

In the developed IB-SEC framework, a security strategy is employed to prevent malevolent activities and provide protected data transmission among the IoT devices, source nodes, and destination nodes using a secure model. The IoT devices are equipped with smart cities and are redirected with secure communication functions. These IoT sensor devices are in constant communication with a higher transmission range over the IoT network to ensure reliable and secure data transmission. Moreover, the source nodes are provided with a private key that is used to create secure data transmission through the destination node. To illustrate, let us consider a monitoring area of 100m x 100m with a data packet size of 50 bits and random deployment. The proposed framework can detect 5 to 25 attacks and use 3 to 15 edge servers, which provide more reliable data transmission. The initial energy of the nodes is set to 5J, and the maximum transmission range towards the IoT network is 20m for simulating various scenarios using MATLAB. Multiple simulation scenarios are generated, and the detection response is recorded and the results are evaluated against the cutting-edge Data Aggregation Routing Protocol (DARP), K-means Clustering Protocol (K-CP), intrusion detection scheme (IDS), Trust management mechanism (TMM) in terms of energy consumption, latency, throughput, and security measure. By implementing these measures, the proposed framework ensures that the data transmission is secure and reliable, which prevents unauthorized access to the transmitted data.

A. PERFORMANCE EVALUATION

The proposed model has been implemented using the MATLAB platform, and the results have been validated against traditional models in terms of energy consumption, security, and throughput. The traditional models used for comparison include the DARP [43], K-CP [44], IDS [28], and TMM [45]. The validation process involves comparing the performance metrics of the proposed model with those of the traditional models, such as energy consumption, security level, throughput, and other relevant parameters. The MATLAB platform is used to setting up the parameters, and running the simulation for the proposed model. The comparison of the proposed model with the traditional models helps to identify the strengths and weaknesses of each model. Based on the results, the proposed model is found to be more efficient and effective than the traditional models in terms of energy consumption, security, and throughput.

1) Energy consumption

Energy consumption is a critical factor to consider in the design of IoT-based smart city applications since IoT devices, ground sensors, and onboard sensors are energy-constrained and battery-operated systems. Energy consumption needs to be minimized as much as possible since a low amount of energy is available to perform specific tasks. Any energy consumed unnecessarily is considered energy wastage. Therefore, reducing the amount of energy utilized by the MAC framework can significantly improve the energy efficiency of the overall system.

Since, energy consumption is an important consideration in IoT-based smart city applications as the IoT devices, ground sensors, and onboard sensors are energy-constrained and battery-operated systems. Low energy consumption is desirable to avoid the wastage of the remaining consumed energy. The proposed IB-SEC strategy has demonstrated improved energy consumption of 0.10334, while the DARP, K-CP, ISD, and TMM models have consumed more energy, such as 0.6j, 0.52j, 0.794j, and 0.43j for 25 IoT nodes, respectively. Similarly, the proposed IB-SEC strategy has demonstrated the lowest energy consumption of 0.3209, while DARP, K-CP, ISD, and TMM have utilized higher energy such as 0.50j, 0.401j, 0.59j, and 0.3299j for 175 IoT nodes. The comparison of the performance is presented in Table 1 and Figure 2.

TABLE 1. The energy consumption measures of the of the proposed IB-SEC and the different state-of-art DARP, K-CP, IDS, and TMM techniques

No.of IoT nodes	Energy consumption (j)				
	DARP	K-CP	IDS	TMM	Proposed IB-SEC
25	0.6	0.51	0.794	0.43	0.10334
50	0.671	0.49	0.74	0.39	0.23822
75	0.63	0.46	0.7	0.38	0.31887
100	0.591	0.452	0.69	0.372	0.32665
125	0.57	0.438	0.6330	0.39069	0.3501
150	0.52	0.422	0.60	0.35	0.333
175	0.50	0.401	0.59	0.3309	0.3299
200	0.45	0.40	0.56	0.32	0.31

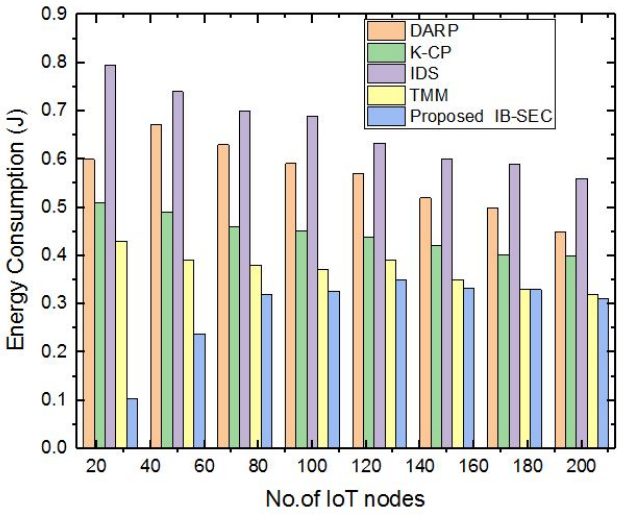

FIGURE 2. A comparison of the energy consumption of the proposed IB-SEC against the DARP, K-CP, IDS, and, TMM

2) Latency

Lower latency is a significant concern in IoT-based smart city applications, particularly when a large amount of data needs to be transferred with minimal delay. Low latency performance is essential for achieving a secure system during the data broadcasting process.

The validation of latency performance was carried out by comparing with existing models such as DARP, K-CP, ISD, and TMM, as shown in table.2 and figure.3. Among these models, DARP processed data within 78.3ms, while K-CP took 67.2ms, which was higher than the other two models. IDS model used 58ms time duration, and TMM utilized 71.03ms. However, the proposed model outperformed all of them by processing the entire performance within 52ms.

3) Throughput

Throughput is an essential measurement factor for data transmission from the source node to the destination node within a given time frame. Developing a secure MAC protocol that

TABLE 2. The latency measures of the of the proposed IB-SEC and the different state-of-art DARP, K-CP, IDS, and TMM techniques

S.No	Technique	Latency (ms)
1	DARP	78.3
2	K-CP	71.2
3	IDS	58
4	TMM	62.03
5	Proposed IB-SEC	51

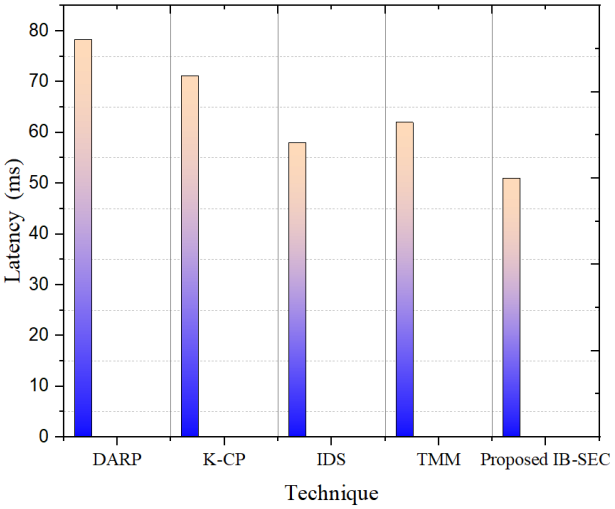

FIGURE 3. A comparison of the latency of the proposed IB-SEC against the DARP, K-CP, IDS, and, TMM

ensures high throughput and efficiency is a vital concern. In smart city applications, the shared information of each IoT device is limited, and hence, a higher throughput is required to manage the millions of IoT devices across the city. In Figure 4 and Table 3, the performance of the proposed IB-ESC model is compared with existing models in terms of throughput. The comparison shows that the DARP model achieved a lower throughput rate compared to other models. Subsequently, the TMM model showed the best performance among the compared models, with a slightly higher throughput rate than the K-CP model. The IDS algorithm achieved an average throughput rate, which was higher than the outcomes provided by both the DARP model. However, the proposed IB-ESC model exceeded all the previous models with a higher throughput rate.

4) Security

Security is a crucial aspect of heterogeneous IoT networks that include both IoT devices and UAVs. In smart cities based on IoT, ensuring the confidentiality of data transmitted from source to destination is essential. The proposed IB-SEC module has been designed to achieve a higher level of security for the IoT network. The security performance of the proposed IB-SEC technique was compared with conventional techniques and the results were illustrated in Table 4 and

TABLE 3. The throughput measures of the proposed IB-SEC and the different state-of-art DARP, K-CP, IDS, and TMM techniques

No.of IoT nodes	Throughput (kbps)				
	DARP	K-CP	IDS	TMM	Proposed IB-SEC
25	24.74	33.54	30.673	45.8912	44.301
50	18.69	20.61	21.42	44.635	22.434
75	14.72	16.671	17.161	43.900	17.242
100	5.821	8.63	7.42	42.6712	9.726
125	3.59	5.52	4.62	40.73	7.23105
150	3.50	5.173	3.56	39.291	6.964
175	3.42	5.376	2.964	38.42	5.76
200	3.3562	4.560	2.2351	37.783	5.241

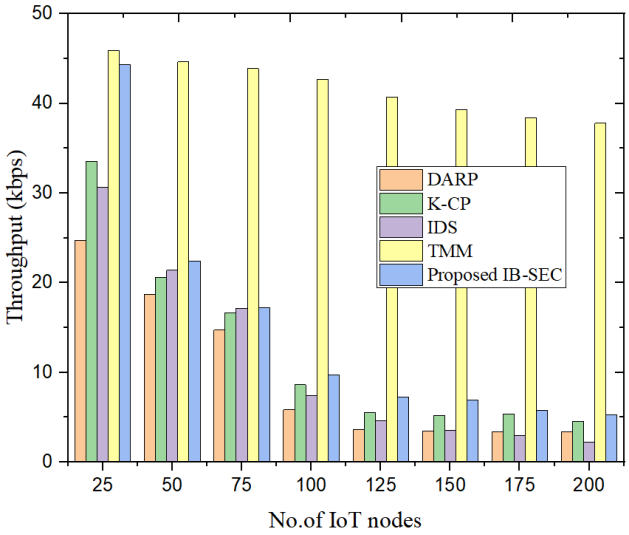

FIGURE 4. A comparison of the throughput of the proposed IB-SEC against the DARP, K-CP, IDS, and, TMM

Figure 5. The graphical representation showed that the IB-SEC approach achieved a higher level of security compared to the other techniques. Specifically, the DARP approach achieved a slightly increased security level over the K-CP approach, while the IDS model obtained a security level closest to the TMM scheme.

TABLE 4. The security measures of the of the proposed IB-SEC and the different state-of-art DARP, K-CP, IDS, and TMM techniques

S.No	Technique	Security (%)
1	DARP	86.11
2	K-CP	91
3	IDS	69.09
4	TMM	72.5
5	Proposed IB-SEC	99

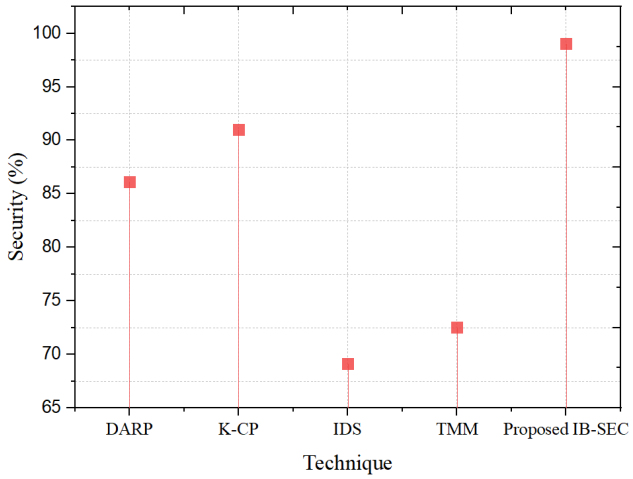

FIGURE 5. A comparison of the security of the proposed IB-SEC against the DARP, K-CP, IDS, and, TMM

TABLE 5. The reliability measures of the of the proposed IB-SEC and the different state-of-art DARP, K-CP, IDS, and TMM techniques

S.No	Technique	Reliability (%)
1	DARP	88
2	K-CP	69.38
3	IDS	79.08
4	TMM	83.7
5	Proposed IB-SEC	98.3

5) Reliability

The reliability of packet delivery is a crucial design parameter for IoT-enabled smart city applications, as it ensures the performance of detecting and recovering from packet drops. Additionally, the reliability performance is affected by the MAC protocol used for data transfer and can have an impact on energy consumption. The reliability of packet delivery is an important design parameter for IoT-enabled smart city applications. It ensures the level of performance by detecting and recovering packet drops. Furthermore, the MAC protocol influences the reliability performance of data transfer and increases energy consumption. The reliability outcomes of the proposed IB-SEC technique were compared with conventional techniques in Table 5 and Figure 6. The graphical representation indicates that the IB-SEC approach achieved a higher level of reliability. DARP achieved slightly higher reliability than K-CP. Similarly, the IDS model obtained a reliability level closest to that of the TMM scheme. Additionally, the state-of-the-art comparison is illustrated in Table 6.

VI. DISCUSSION

In DARP methods [43], a smaller number of nodes are involved in the performance of data transmission, which also results in reduced congestion on the routing pathways and little contention on wireless networks. The strength of wireless

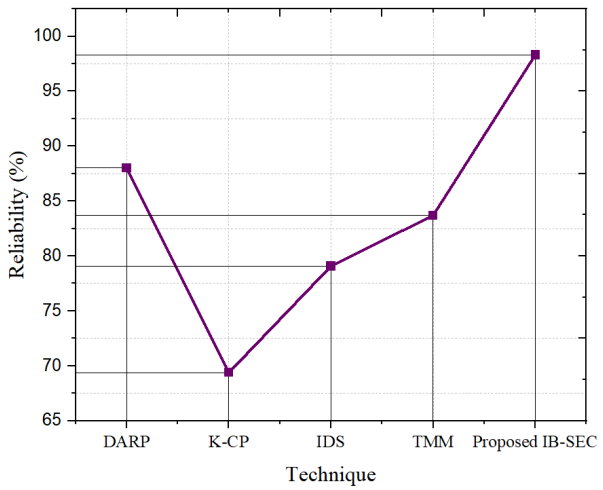

FIGURE 6. A comparison of the Reliability of the proposed IB-SEC against the DARP, K-CP, IDS, and TMM

connections is also evaluated based on the network condition to prolong the lifetime of the routing path. The security problem and energy consumption problems are lacking in K-CP [44] analysis. The IDS [28] method in edge computing has a high risk of false alarm; it only considered the intrusion in the network due to the lacking of attack prevention. The IDS method has achieved very high energy consumption and very less throughput compared with the other methods. Poor witnesses and internal mistakes both have an impact on the node's ability to manage trust using TMM [45]. The proposed method has achieved superior performance in terms of reduced energy consumption, latency, and improved throughput, security, and scalability. The proposed algorithm has an intelligent function thus a high amount of attacks can able to detect. The high throughput and security value show the effective data transmission and confidentiality of varying IoT applications. The security requirement and energy consumption are ensured by the graphical analysis of this research. However, one of the limitations of this work is that the experimental setup is confined to a specific area, with limited data packet sizes, uncertainties in the IoT data [46, 47], and a restricted number of attacks on the IoT-based network. For a more realistic scenario, future work should consider a larger network size and diverse packet sizes, as well as a range of various types of attacks, from data injection to DDoS attacks.

VII. CONCLUSION

In this paper, we proposed the IB-SEC platform, which is a promising solution for enhancing the performance of IoT networks in smart cities. By leveraging secure edge computing and adaptive MAC protocols, the platform can efficiently integrate heterogeneous devices and systems, while addressing key concerns such as energy consumption, reliability, and security. The platform's ability to dynamically adapt to changing network conditions and traffic loads enables it to achieve higher throughput, lower latency, and improved packet delivery reliability, thereby enhancing the overall efficiency of IoT networks in smart cities. Results indicate that edge servers' lower latency has a considerable positive impact on energy consumption. The proposed IB-SEC platform has shown notable advancements in its ability to effectively minimize overall task latency with expanding data and subdivisions, minimize energy consumption, and offer significant security to IoT networks in smart cities. Specifically, the developed model has achieved a lower energy consumption of 0.32j and a lower latency of 51ms for a given number of IoT nodes. Moreover, the proposed approach has attained the highest security level and a high detection rate, effectively repelling hacker attempts through the use of advanced MAC protocols. The achieved results of the proposed approach have been compared with existing methodologies, highlighting the superior efficiency and effectiveness of the proposed model. Overall, the IB-SEC platform represents a significant advancement in secure edge-enabled computing, providing a robust and reliable solution for managing the diverse requirements of smart city devices while ensuring the secure transmission of data. The use of supervised machine learning techniques for routing will be something we experiment with in the future, along with the addition of node attributes other than those employed in this study. In summary, the proposed platform enables efficient data acquisition, preprocessing, and analysis while ensuring the security and privacy of the data. While the experimental setup has limitations, it provides a solid foundation for future research in this area. However, there are several open challenges that need to be addressed in future work, such as support for Quality-of-Service (QoS), performance, and the impact of load distribution on the servers. By addressing these challenges, we aim to develop a cost-effective and sustainable communication infrastructure that can support the growing demand for IoT devices in smart cities.

ACKNOWLEDGMENT

The authors are thankful to the Deanship of Scientific Research at Najran University for funding this work, under the General Research Funding program grant code (NU/DRP/SERC/12/11).

This publication has also emanated from research supported in part by a grant from Science Foundation Ireland under Grant Number SFI/16/RC/3918 (Confirm), and also by a grant from SFI under Grant Number SFI 12/RC/2289_P2 (Insight). For the purpose of Open Access, the author has applied a CC BY public copyright license to any Author Accepted Manuscript version arising from this submission.

REFERENCES

[1] Muhammad Faisal, Rashid Mehmood, and Abid Ali Minhas. Smart city and IoT: An overview, opportunities, and future directions. Sensors, 19(15):3358, 2019.

[2] Shuyan Jiang, Qiang Yu, Xiaoyu Chen, Liang Chen, and Xiaoguang Zhang. The application of IoT, big data,

and artificial intelligence technologies in smart cities: A review. Journal of Sensors, 2021:1–20, 2021.

[3] Junaid Qadir and et al. Smart cities: Concept, challenges, and future directions. Journal of Communications and Networks, 20(5):399–413, 2018.

[4] Tang Lei, Zhu Cai, and Luo Hua. 5g-oriented IoT coverage enhancement and physical education resource management. Microprocessors and Microsystems, 80:103346, 2021.

[5] Edna Iliana Tamariz-Flores and Richard Torrealba-Meléndez. Vehicular network systems in smart cities. In Handbook of Smart Cities, pages 721–749. Springer International Publishing, Cham, 2021.

[6] Muhammad Adil and Muhammad Khurram Khan. Emerging IoTapplications in sustainable smart cities for covid-19: Network security and data preservation challenges with future directions. Sustainable Cities and Society, 75:103311, 2021.

[7] Samir Dawaliby, Abbas Bradai, and Yannis Pousset. Joint slice-based spreading factor and transmission power optimization in lora smart city networks. Internet of Things, 14:100121, 2021.

[8] Amjad Rehman, Khalid Haseeb, Tanzila Saba, and Hoshang Kolivand. M-smdm: a model of security measures using green internet of things with cloud integrated data management for smart cities. Environmental Technology & Innovation, 24:101802, 2021.

[9] Nasaruddin F. Gani A. Karim A. Hashem I.A.T. Siddiqa A. Marjani, M. and Yaqoob. Big IoT data analytics: architecture, opportunities, and open research challenges. IEEE Access, 5:5247–5261, 2017.

[10] ADI Alhudhaif, Musheer Ahmad, Ahmed Alkhayyat, Nestor Tsafack, Alaa Kadhim Farhan, and Rafeeq Ahmed. Block cipher nonlinear confusion components based on new 5-d hyperchaotic system. IEEE Access, 9:87686–87696, 2021.

[11] Sabbir Ahmed, Md Farhad Hossain, M Shamim Kaiser, Manan Binth Taj Noor, Mufti Mahmud, and Chinmay Chakraborty. Artificial intelligence and machine learning for ensuring security in smart cities. In Data-Driven Mining, Learning and Analytics for Secured Smart Cities: Trends and Advances, pages 23–47. Springer, 2021.

[12] Ammar Mohammed Ali and Alaa Kadhim Farhan. A novel improvement with an effective expansion to enhance the md5 hash function for verification of a secure e-document. IEEE Access, 8:80290–80304, 2020.

[13] Nahla Nurelmadina, Omar Alsaiari, Bilal B Zaidan, Ameerah N Zaidan, OS Albahri, AH Alamoodi, AS Albahri, AS Albahri, Faisal Almehmadi, and Kim-Kwang Raymond Choo. A systematic review on cognitive radio in low power wide area network for industrial IoT applications. Sustainability, 13(1):338, 2021.

[14] Javed Ashraf, Marwa Keshk, Nour Moustafa, Mohamed Abdel-Basset, Hasnat Khurshid, Asim D Bakhshi, and Reham R Mostafa. IoTBoT-IDS: A novel statistical learning-enabled botnet detection framework for protecting networks of smart cities. Sustainable Cities and Society, 72:103041, 2021.

[15] Usman Khalil, Owais Ahmed Malik, Saddam Hussain, et al. A blockchain footprint for authentication of IoT-enabled smart devices in smart cities: State-of-the-art advancements, challenges and future research directions. IEEE Access, 10:76805–76823, 2022.

[16] MAAJ Ali Alaa K Farhan. Database protection system depend on modified hash function. Conference of Cihan University-Erbil on Communication Engineering and Computer Science, page 84, 2017.

[17] P Muralidhara Rao and BD Deebak. Security and privacy issues in smart cities/industries: Technologies, applications, and challenges. Journal of Ambient Intelligence and Humanized Computing, pages 1–37, 2022.

[18] Shahbaz Siddiqui, Sufian Hameed, Syed Attique Shah, Abdul Kareem Khan, and Adel Aneiba. Smart contract-based security architecture for collaborative services in municipal smart cities. Journal of Systems Architecture, 135:102802, 2023.

[19] Muhammad Zulkifl Hasan and Zurina Mohd Hanapi. Efficient and secured mechanisms for data link in IoT WSNs: A literature review. Electronics, 12(2):458, 2023.

[20] Vasiliki Demertzi, Stavros Demertzis, and Konstantinos Demertzis. An overview of cyber threats, attacks and countermeasures on the primary domains of smart cities. Applied Sciences, 13(2):790, 2023.

[21] Hassan Zeb, Moneeb Gohar, Moazam Ali, Waleed Ahmad, Anwar Ghani, Jin-Ghoo Choi, Seok-Joo Koh, et al. Zero energy IoT devices in smart cities using rf energy harvesting. Electronics, 12(1):148, 2023.

[22] Lei Liu, Yan Wang, Guangjie Han, Jiannong Cao, and Joel J. P. C. Rodrigues. A survey of mac protocols for smart city applications. IEEE Communications Surveys & Tutorials, 22(3):1616–1646, 2020.

[23] Zhirong Xu, Ming Cai, Xiaoyan Li, Tianlei Hu, and Qianshu Song. Edge-aided reliable data transmission for heterogeneous edge-IoT sensor networks. Sensors, 19(9):2078, 2019.

[24] Jin Wang, Yu Gao, Wei Liu, Arun Kumar Sangaiah, and Hye-Jin Kim. An improved routing schema with special clustering using pso algorithm for heterogeneous wireless sensor network. Sensors, 19(3):671, 2019.

[25] Md Arafatur Rahman, A Taufiq Asyhari, LS Leong, GB Satrya, M Hai Tao, and MF Zolkipli. Scalable machine learning-based intrusion detection system for IoT-enabled smart cities. Sustainable Cities and Society, 61:102324, 2020.

[26] Zhiwei Zhao, Geyong Min, Weifeng Gao, Yulei Wu, Hancong Duan, and Qiang Ni. Deploying edge computing nodes for large-scale IoT: A diversity aware approach. IEEE Internet of Things Journal, 5(5):3606–3614, 2018.

[27] Sura Khalaf Alaa Kadhim. New approach for security

chatting in real time. Int. J. Emerg. Trends Technol. Comput. Sci., 4:30–36, 2015.

[28] Ayesha Altaf, Haider Abbas, Faiza Iqbal, Malik Muhammad Zaki Murtaza Khan, Abdul Rauf, and Tehsin Kanwal. Mitigating service-oriented attacks using context-based trust for smart cities in IoT networks. Journal of Systems Architecture, 115:102028, 2021.

[29] Hassan R Yassein, Nadia MG Al-Saidi, and Alaa K Farhan. A new ntru cryptosystem outperforms three highly secured ntru-analog systems through an innovational algebraic structure. Journal of Discrete Mathematical Sciences and Cryptography, 25(2):523–542, 2022.

[30] Mehdi Gheisari, Hamid Esmaeili Najafabadi, Jafar A Alzubi, Jiechao Gao, Guojun Wang, Aaqif Afzaal Abbasi, and Aniello Castiglione. Obpp: An ontology-based framework for privacy-preserving in IoT-based smart city, 2021.

[31] Ahmed A Abd El-Latif, Bassem Abd-El-Atty, Irfan Mehmood, Khan Muhammad, Salvador E Venegas-Andraca, and Jialiang Peng. Quantum-inspired blockchain-based cybersecurity: securing smart edge utilities in IoT-based smart cities. Information Processing & Management, 58(4):102549, 2021.

[32] Mikail Mohammed Salim, Sushil Kumar Singh, and Jong Hyuk Park. Securing smart cities using lstm algorithm and lightweight containers against botnet attacks. Applied Soft Computing, 113:107859, 2021.

[33] A Duraisamy and M Subramaniam. Attack detection on IoT based smart cities using ids based manfis classifier and secure data transmission using irsa encryption. Wireless Personal Communications, 119:1913–1934, 2021.

[34] Zhichao Zheng, Jianhua Li, Yan Wang, and Shaoqian Wu. Survey of reinforcement-learning-based mac protocols for wireless ad hoc networks with a mac reference model. Entropy, 25(1):101, 2023.

[35] S Nagaraj, Atul B Kathole, Leena Arya, Neha Tyagi, SB Goyal, Anand Singh Rajawat, Maria Simona Raboaca, Traian Candin Mihaltan, Chaman Verma, and George Suciu. Improved secure encryption with energy optimization using random permutation pseudo algorithm based on internet of thing in wireless sensor networks. Energies, 16(1):8, 2023.

[36] Alaa Kadhim Farhan Ammar Mohammed Ali. A novel improvement with an effective expansion to enhance the md5 hash function for verification of a secure e-document. IEEE Access, 8:80290–80304, 2020.

[37] Yossra Hussain Ali, Seelammal Chinnaperumal, Raja Marappan, Sekar Kidambi Raju, Ahmed T Sadiq, Alaa K Farhan, and Palanivel Srinivasan. Multi-layered non-local bayes model for lung cancer early diagnosis prediction with the internet of medical things. Bioengineering, 10(2):138, 2023.

[38] Hakeem Imad Mhaibes, May Hattim Abood, and Alaa Kadhim Farhan. Simple lightweight cryptographic algorithm to secure imbedded IoT devices. International Journal of Interactive Mobile Technologies, 16(20), 2022.

[39] Abeer Tariq Maolood Fahimeh Nazarimehr Iqtadar Hussain Alaa Kadhim Farhan, Nadia MG Al-Saidi. Entropy analysis and image encryption application based on a new chaotic system crossing a cylinder. Entropy, 21:958, 2019.

[40] Balvender Singh, SK Bishnoi, Mandeep Sharma, Pushpendra Singh, and Sandeep Dhundhara. An application of nature inspried algorithm based dual-stage frequency control strategy for multi micro-grid system. Ain Shams Engineering Journal, page 102125, 2023.

[41] Alaa K. Farhan Hassan R. Yassein, Nadia M. G. Al-Saidi. A new ntru cryptosystem outperforms three highly secured ntru-analog systems through an innovational algebraic structure. Journal of Discrete Mathematical Sciences and Cryptography, pages 523–542, 2020.

[42] Rasha Subhi Alin F Alaa Kadhim, Ghassan H Abdul-Majeed. Enhancement cast block algorithm to encrypt big data. 2017 Annual Conference on New Trends in Information Communications Technology Applications (NTICT), pages 80–85, 2017.

[43] Khalid Haseeb, Naveed Islam, Tanzila Saba, Amjad Rehman, and Zahid Mehmood. Lsdar: A light-weight structure based data aggregation routing protocol with secure internet of things integrated next-generation sensor networks. Sustainable Cities and Society, 54:101995, 2020.

[44] Deepak Kumar Sharma, Sanjay Kumar Dhurandher, Divyansh Agarwal, and Kunal Arora. krop: k-means clustering based routing protocol for opportunistic networks. Journal of Ambient Intelligence and Humanized Computing, 10:1289–1306, 2019.

[45] Kamran Ahmad Awan, Ikram Ud Din, Ahmad Almogren, Hisham Almajed, Irfan Mohiuddin, and Mohsen Guizani. Neurotrust—artificial-neural-network-based intelligent trust management mechanism for large-scale internet of medical things. IEEE Internet of Things Journal, 8(21):15672–15682, 2020.

[46] Shahid Hussain, Subhasis Thakur, Saurabh Shukla, John G Breslin, Qasim Jan, Faisal Khan, and Yun-Su Kim. A two-layer decentralized charging approach for residential electric vehicles based on fuzzy data fusion. Journal of King Saud University-Computer and Information Sciences, 34(9):7391–7405, 2022.

[47] Shahid Hussain, Mohamed A Ahmed, and Young-Chon Kim. Efficient power management algorithm based on fuzzy logic inference for electric vehicles parking lot. IEEE Access, 7:65467–65485, 2019.

REYAZUR RASHID IRSHAD received the B.Sc. degree from Aligarh Muslim University, Aligarh, India, in 2000, and the master's degree in computer application from Indira Gandhi University, New Delhi, India in 2010. He is currently pursuing a Ph.D. degree at JJT University, Rajasthan. He is also a Lecturer at the Department of Computer Science, Najran University, Saudi Arabia. He has published many articles in reputed journals and has attended some conferences. His research interest includes web-based applications.

SHAHID HUSSAIN received a BS in Mathematics and an M.Sc in Computer Science from the University of Peshawar in 2002 and 2005, respectively. He obtained his MS and Ph.D. in Computer Engineering from Jeonbuk National University in South Korea in 2016 and 2020, respectively. He achieved the Jeonbuk National University presidential award for academic excellence during his Ph.D. studies. He was a postdoctoral researcher at the Gwangju Institute of Science and Technology (GIST) in South Korea (2020) and the University of Galway (UoG) in Ireland from 2020 to 2022. He is currently working as a senior postdoctoral researcher at the Innovative Value Institute (IVI), School of Business, National University of Ireland Maynooth (NUIM), Ireland. His research interests include smart grid, energy management, electric vehicles, smart grid infrastructure, optimization algorithms, Micro-grid operations, distributed energy resources, Peer-to-peer energy trading, and machine learning in medical applications (e.g. prediction and risk analysis of osteoporosis) using fuzzy logic, game theory, ontology, AI, and blockchain approaches and technologies.

IHTISHAM HUSSAIN is a student at the Abdul Wali Khan University of Mardan in KPK, Pakistan, where he is pursuing a BS in computer science. He has participated in several coding competitions, hackathons, internships, and projects. Besides his academic interests, he is a devoted programmer and technology enthusiast, continuously investigating new tools and approaches to enhance his coding talents. His research interests include artificial intelligence and machine learning applications in a variety of fields such as bioinformatics, energy, and business

IBRAR AHMAD is an Assistant Professor in the Department of Computer Science at University of Swat, KPK, Pakistan. He received his bachelor's degree in Computer Science from the University of Peshawar, Pakistan, in 2006, and completed his Master's degree in Engineering Management from the Seoul National University (SNU), Republic of Korea, in 2016. He obtained a PhD degree in the Information Telecommunication Technology Program, at Korea Advanced Institute of Science and Technology (KAIST), Republic of Korea. His research interests are IT Management, Smart Agriculture, Rural Telecommunications Infrastructure, and Information system.

ADIL YOUSIF received the B.Sc. and M.Sc. degrees from the University of Khartoum, Sudan, and the Ph.D. degree from the University of Technology in Malaysia (UTM). He is currently an Associate Professor at the College of Arts and Sciences Sharourah, Najran University, Saudi Arabia. He is also the principal investigator of several research projects in artificial intelligence and emerging technologies. His research interests include computer networks, cloud computing, artificial intelligence, and optimization techniques.

IBRAHIM M. ALWAYLE received his B.Sc. in Mathematics from San'aa University, Yemen in 1999, and M.Sc. and Ph.D. in computer science from Al Mansurah University, Egypt in 2004, 2008 respectively. He is an assistant professor in the Department of computer science at Najran University, KSA. He is permanently an assistant professor in Amran University, Yemen. His research focuses on pattern recognition, image processing, and AI.

AHMED ABDU ALATTAB received the B.Sc. degrees in computer science from the University of Baghdad, Baghdad, Iraq, in 1997, the M.Sc. degree in computer science from the University of Technology, Baghdad, Iraq, in 2002 and the Ph.D. degree in computer science-artificial intelligence from the University of Malaya, Kuala Lumpur, Malaysia, 2013. He is currently an Assistant Professor at the Department of Computer Science, Najran University, Saudi Arabia. He is also an Assistant Professor at Thamar University, Yemen. He has published many articles in reputed journals and conferences. His research interests include artificial intelligence image processing, image retrieval, image classification, object recognition, deep learning, natural language processing, computer vision, and neural networks.

KHALED M. ALALAYAH received the B.Sc. and M.Sc. degrees in computer science from the University of Technology, Baghdad, Iraq, in 1999 and 2003, respectively, and the Ph.D. degree from Menoufia University, Egypt, in 2011. He is currently an Assistant Professor with the Department of Computer Science, at Najran University, Saudi Arabia. He is also an Assistant Professor at Ibb University, Yemen. He has published many articles in reputed journals and conferences. His research interests include information security, data mining, image processing, and neural networks.

JOHN BRESLIN is a Personal Professor (Personal Chair) in Electronic Engineering at the College of Science and Engineering at the National University of Ireland Galway, where he is Director of the TechInnovate / AgInnovate programmes. John has taught electronic engineering, computer science, innovation, and entrepreneurship topics during the past two decades. Associated with three SFI Research Centres, he is a Co-Principal Investigator at Confirm (Smart Manufacturing) and Insight (Data Analytics), and a Funded Investigator at VistaMilk (AgTech). He has written 200+ peer-reviewed academic publications (h-index of 42, 7400 citations, best paper awards from IoT, DL4KGS, SEMANTiCS, ICEGOV, ESWC, PELS), and co-authored the books "Old Ireland in Colour", "The Social Semantic Web" and "Social Semantic Web Mining". He co-created the SIOC framework (Wikipedia article), implemented in hundreds of applications (by Yahoo, Boeing, Vodafone, etc.) on at least 65,000 websites with 35 million data instances

MOHAMMED MEHDI BADR received his B.Sc. in 1992 from Damietta University, (Mansurah University), Egypt , and M.Sc. and PhD in computer science from Damietta University (Mansurah University), Egypt in 2000 , 2010 respectively. He is an assistant professor in the Department of Computer Science at Najran University, KSA. He is permanently lecturer in College of Computers and Artificial Intelligence, department of computer science at Damietta University, Egypt. His research focuses on Natural language processes on Machine learning, Neural networks , IOT, AI.

JOEL J. P. C. RODRIGUES (Fellow, IEEE) is currently with the College of Computer Science and Technology, China University of Petroleum (East China), China, and the Senac Faculty of Ceará, Brazil, and a Senior Researcher at the Instituto de Telecomunicações, Portugal. He has authored or coauthored more than 1000 papers in refereed international journals and conferences, three books, two patents, and one ITU-T recommendation. He is a member of the Internet Society, a Senior Member of ACM, and a fellow of AAIA. He is also the Leader of the Next Generation Networks and Applications (NetGNA) Research Group, CNPq, and a Representative Member of the IEEE Communications Society on the IEEE Biometrics Council. He is the Editor-in-Chief of the International Journal of E-Health and Medical Communications and a editorial board member of several journals. He was the Director of the Conference Development-IEEE ComSoc Board of Governors, an IEEE Distinguished Lecturer, a Past Chair of the IEEE ComSoc TCs on eHealth and on Communications Software, and a Steering Committee Member of the IEEE Life Sciences Technical Community.