



INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Secure Data Collection Model in IOT

Aayush Pratap Singh^{#1}, Dr.Sanjay Kumar Yadav^{*2}

1 Department of Computer Science & IT, SHUATS, Prayagraj, India.

2 Associate Professor, Department of Computer Science & IT, SHUATS, Allahabad, India

Abstract: Edge computing and the Internet of Things (IoT) have not only revolutionised the manner in which data is managed and analysed, but they have also made it feasible to decrease latency while simultaneously improving energy efficiency. This is a significant development. However, there is still a significant amount of work that needs to be done in order to ensure that these systems are safe and that their data integrity is preserved. The research that is being presented here proposes a one-of-a-kind approach that has the potential to effectively address these issues within the framework of edge computing and the internet of things. Base64 encoding, trustworthy algorithms, and virtual force mapping depending on trust value are all components that are included in this implementation. This design not only enhances security and dependability by giving precedence to components that are trustworthy and safeguarding data while it is being sent, but it also makes a significant contribution to the reduction of energy consumption, which is a major benefit for all parties involved. The approach that has been described has been shown to provide a powerful solution for the processing of data in edge computing and Internet of Things systems that is reliable, efficient, and safe. This has been demonstrated via the presentation of the method. Because of this, it paves the way for future expansion and development in these sectors, which is a result of this.

Keywords- Security; Edge Computing; WSN; Encryption

Introduction

Because of the quick rise of edge computing and the Internet of Things (IoT), there has been a remarkable increase in the number of devices that are connected to the internet. This is a direct result

of the rapid growth of both of these technologies. In order to ensure the safety and effectiveness of the management of the massive volumes of data that are generated by these devices, it is essential to have a system in place [1-2]. A variety of advantages are made available to the individuals who make use of these recently developed technologies. These advantages include a reduction in latency, an improvement in energy economy, and an enhancement in decision-making abilities. However, the rise in the number of devices and sources of data is accompanied by an increase in the problems that are associated with maintaining the integrity of the data [3]. This is because the number of devices and sources of data continued to expand. There is a need for innovative ways that are capable of maintaining the security and reliability of data in situations such as edge computing and the internet of things [4-5]. This is necessary in order to discover answers to the problems that have been identified.

Based on the findings of this research, a framework that is completely unique has been established. This framework combines base64 encoding with virtual force mapping that is based on trust value. The solutions for edge computing and the Internet of Things were the primary motivation for the development of this framework. This research is intended to examine the questions that have been brought up in order to offer answers to those issues. Our objective is to execute this technology in such a way that not only will we be able to achieve significant reductions in the amount of energy that we use, but we will also be able to significantly improve the dependability of the system, the trustworthiness of the data, and the security of the data. This is our goal. In the process of developing this technology, edge computing and devices

connected to the Internet of Things were taken into consideration. For the purpose of achieving the goal of improving data security and trustworthiness, the framework that has been constructed has been intended to give more priority to components that have higher trust levels and to secure data while it is being sent by using base64 encoding. We are able to accomplish large reductions in the amount of energy that is required by edge computing and Internet of Things ecosystems by using this technology. Not only are we able to increase the safety and reliability of data, but we are also able to achieve these reductions. Because of this, we are able to improve the reliability of the data as well as provide it with more security. The dependable path that leads to the selection of nodes is shown in Figure 1.

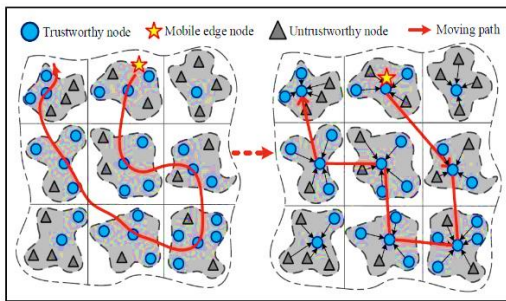


Fig. 1 Trustworthy Node Selection [1]

Base64 encoding, the concept of virtual force mapping by trust value, and the integration of these techniques within the framework of edge computing and the Internet of Things (IoT) are all topics that will be discussed in further detail in the subsequent parts of this article. In addition, we will discuss the benefits that this new framework offers, as well as the implications that it has for the effectiveness of energy utilisation via its implementation.

Experiment and Simulation

To developing a trustworthy algorithm that addresses the challenges of data security, trustworthiness, and system dependability in situations involving edge computing and the Internet of Things, we may characterise the problem as follows:

The objective is to provide a framework (F) that, when provided with a collection of edge devices (E), data sources (D), and algorithms (A), as well as the trust values (T) that are connected with them, is capable of performing the following tasks: The base64 encoding technique should be used to encrypt any sensitive information before sending it across insecure channels. This will prevent unauthorised access to the data as well as

alteration of the data. Compute trust values (T) for each component, including edge devices, data sources, and algorithms, by considering factors such as the reputation of the device, its track record of performance, and the security regulations that are already in place. The trust values (T) in edge computing and Internet of Things (IoT) systems should be mapped to a virtual force (V) that has an effect on the selection and prioritisation of components (E, D, and A) for processing tasks. In order to create a system that is more trustworthy and reliable, it is necessary to assign duties to the components that have been selected, taking care to provide greater priority to those components that can be depended upon the most. The performance of the system may be improved by reducing the amount of time it takes for data to be processed and the amount of energy it consumes, all while ensuring that the system's integrity and the security of user information are preserved. The final objective is to design a complete framework (F) that unifies base64 encoding, trust value computation, virtual force mapping, and job allocation in order to guarantee the security, trustworthiness, and dependability of edge computing and Internet of Things (IoT) systems while simultaneously reducing the amount of energy that is used. In the shortest amount of time feasible, this will be completed.

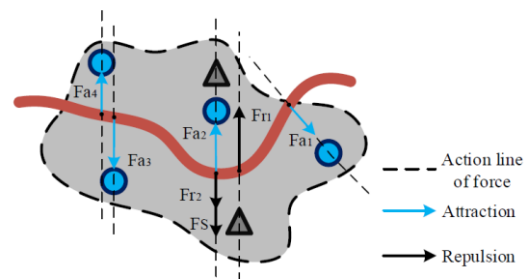


Fig. 2 Trust Action Forces in VFDC [1]

Through the use of the mathematical model, we are able to simulate a wide range of situational scenarios. There might be a varied number of edge devices, data sources, algorithms, and tasks involved in these situations. Furthermore, we are able to test the model in a range of situations, such as comparing methods for computing trust values, functions for virtual force mapping, and task allocation procedures. This is another capability that we possess.

By conducting a study of the performance metrics, we will be able to establish the extent to which the proposed framework is effective in reducing energy consumption in edge computing and Internet of Things settings, as well as improving data security, trustworthiness, and

system stability. It will be much simpler to demonstrate the superiority of the trustworthy algorithm that has been provided if the outcomes are compared with methods that are presently being used.

Related Work

The typical architecture of centralised cloud computing is facing a number of significant issues that are now being faced. The necessity to expand in order to fulfil the growing demand for mobile broadband and applications for the Internet of Things (IoT) is one of the obstacles that must be overcome. The amount of strain that is placed on radio access networks (RANs) and backhaul networks, as well as the amount of time it takes for data to travel between nodes, both rise when mobile devices are linked to remote cloud servers that are centralised. This is done in order to download complicated software. The Internet of Things (IoT) is also driving a digital revolution in a range of sectors of contemporary modern life [2, 3]. This is possible due to the constantly growing number of access devices as well as the expectations of end-users. The field of healthcare is one of these fields. [3]: According to projections, the Internet of Things will connect fifty billion devices by the year 2020, with mobile phones constituting the vast bulk of these connections. The projections in question come from Cisco. As the Internet of Things (IoT) continues to expand at a rapid pace, it presents new challenges that the architecture of centralised cloud computing is unable to fully solve. Some of these problems include high levels of latency, capacity constraints, devices that are fueled by renewable energy, continuous service despite delays in the network, and enhanced levels of security. [4] Sensor nodes are dispersed at random throughout desert regions and dangerous surroundings in order to accomplish a wide variety of difficult jobs in a great number of different conditions. It is because of this that the nodes are able to carry out a broad range of labor-intensive activities. (5)–(7) One of the numerous uses for sensor nodes is the surveillance of battlefields; other applications include the monitoring of smart cities, the monitoring of medical problems, the identification of illegal entrances, and the provision of emergency response. The complex environment in which the underlying sensor network operates makes it more susceptible to being penetrated by malicious actors. This puts the network at a greater risk of being compromised. This is due to the fact that the context makes it more likely that it will be

corrupted. This is a direct result of the fact that sensors gather information that is either inaccurate or completely created in order to be deceitful. The fact that fewer than 49 percent of the data are reliable and accurate is another factor that contributes to the high danger that is posed by the situation [8]. It is [9]. If the process of gathering data via sensor networks is difficult and unreliable, then doing it at higher levels of data security and application will be far more complex, and it is very unlikely that it will be successful. Network security is the practice of securing network systems or network resources against unauthorised access of any kind, including intrusions that are carried out on purpose as well as those that occur accidentally [10]. The word "network security" includes both intentional and accidental intrusions. With regard to the underlying wireless sensor networks (WSNs), it is feasible to categorise the assault as either an internal or an external attack, depending on the origin of the attack [11]. An internal attack is an assault that originates inside the Wireless Sensor Network (WSN) itself. This kind of attack is known to by its term, "internal attack." Internal attacks on the underlying network that constitutes the Internet of Things are not only far more damaging than external attacks [12], but they are also significantly cheaper. This is something that has been shown to be true while looking back at the past. Furthermore, even if the security procedures for cryptographic authentication and routing protocols are successful in preventing attacks from the outside, they are not successful in preventing attacks from inside the organisation. This is the case regardless of whether or not the processes that are being followed successfully. This is a significant distinction between the two types of attacks that have been detailed that have been discussed. By carrying out a trust assessment, it is feasible to deal with hostile nodes that are contained inside a node in a fashion that is both straightforward and efficient [13, 14]. In spite of the fact that this is taking place, it is very essential that you keep this degree of security on your computer.

Implementation

The challenge that has been presented here is now being addressed by the creation of a solution that is currently in the process of being constructed. One method that takes use of edge computing in order to collect data from reliable nodes is the one that is being discussed here. Because of this, it will be simple to avoid dealing with the problem

that has been brought up because of this. Within the scope of this body of work, the calculation of trust may include the use of both direct and indirect methodologies. In the event that the sensor is placed within the range of its cluster head, the direct technique will be utilised, while the indirect approach will be utilised in the event that the sensor is situated that is outside of the range of its cluster head. It is possible to use each of these tactics in conjunction with one another so that you may get your desired results. It is possible to achieve the objectives that have been established by using a strategy that involves the utilisation of each of these methods in combination with these other strategies. The evaluation of trust within the confines of the subject matter of this study may be accomplished via the use of either direct or indirect techniques; both of these approaches are valid alternatives. In the event that the sensor is positioned inside the field of vision of the cluster head, the direct approach will be used in the event that this happens.

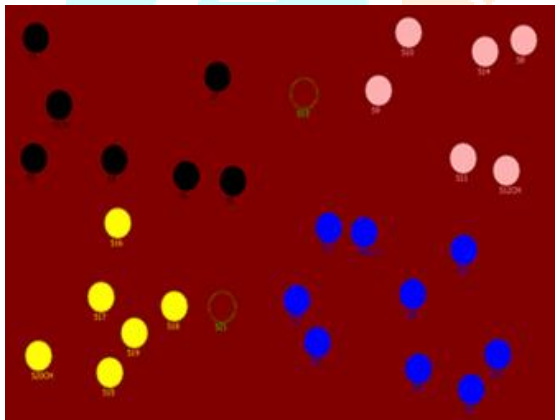


Fig. 3 Network Simulation Setup

When it comes to this particular investigation, the default trust value for each of the nodes is established to be 0.5. The cluster head is the person who has the power to either enhance or decrease the trust value of individual nodes, based on the conduct of the other nodes that are part of the cluster. It is possible for them to do this by watching the behaviour of the nodes inside the cluster. To put it another way, the default degree of trust that is allocated to each of the nodes is 0.5, but they are the ones who have the ability to adjust this number in any way that they see to be suitable. It is the results that were collected from the study that would serve as the basis for the value that was acquired as a result of this. If every single packet that originates from a particular node is sent to the cluster head, then the trust value of that node will increase as a consequence of this. Furthermore, this holds true for sensors in addition to nodes. This is due to the fact that the

member of the network who is given the highest level of confidence is the leader of the cluster. This is the reason why things are the way they are. When this does not take place, the trust value of the node will decline, which is in contrast to what would happen if this were to take place. In the event that it did take place, this is the opposite of what would take place. For the purpose of determining whether or not an individual need to put their trust in another person, a number of different force metrics, including the amount of energy that is utilised, the distance that separates the two parties, and the quality of the data, are employed in combination with several other metrics. One of the reasons for this is to guarantee that the picture that is acquired is as accurate as it is possible to hope for. In the case that a node is positioned in such a manner that it is in close proximity to the cluster head and consumes less energy than the average of the other nodes, then the data quality will be exceptional, and as a result, the trust value of the data will grow. This is because the cluster head is in close proximity to the node.

Edge computing is a relatively new technology that brings the processing of data closer to the site where it was created. The name "edge computing" will be used to describe this technology. One of the most important benefits of edge computing is that it eliminates the need to transport data between edge devices and the cloud. This is one of the reasons why edge computing is becoming more prominent. Consequently, this leads to a decrease in the amount of network capacity that is used, an increase in responsiveness, and a reduction in the amount of delay that occurs. However, in addition to these advantages, there are additional issues that need to be answered in terms of the reliability and security of the data. These challenges need to be addressed.

The purpose of the Base64 encoding system, which is in charge of transforming binary data to text, is to encode binary data in a string format that is based on the ASCII alphabet. This is the system's primary objective. Encoding data for the purpose of transmission across protocols that are only capable of processing text-based data, such as email or HTTP, is one of the most prevalent uses of this encoding method. This encoding technique is used to encode data for the purpose of transmission.

The data that is being sent between edge devices and the central cloud, or even between edge devices themselves, may be encrypted using base64 encoding in order to ensure that it is secure. This is done in the context of edge computing. It is a simplistic method that, contrary

to appearances, is very effective when it comes to preventing unauthorised access to or modification of sensitive data. This encoding technique gives an easy strategy that is highly successful.

Evidence that the Algorithm is of Acceptable Quality A Comprehensive Mapping of the Virtual Force, Using Trust Values as the Reference Point The trustworthy algorithm virtual force, which is often referred to by its acronym, TAVF, is a revolutionary idea that intends to improve the dependability and safety of edge computing settings. If you are interested in learning more about this concept, go here. It is a process that includes mapping trust values to different components of the system, such as edge devices, data sources, and algorithms, in order to evaluate the trustworthiness of these components. In this context, an algorithm is an example of such a component.

The Application of Computational Methods to Trust Values It is this Several variables are taken into account in order to ascertain the degree of trust that exists between two parties. The reputation of the gadget, its previous performance, and the security measures that have been developed at this time are all included in these factors. Whenever there is new information that has to be taken into consideration, these values are subject to alterations that are both regular and dynamic.

The Methodology Behind the Mapping of Trust Values to a Virtual Agency: When using this approach, trust values are mapped to a virtual force, which then acts as a guide for the selection of edge devices, data sources, and algorithms for the purpose of carrying out processing tasks. The possibility of a person being selected for a certain task is boosted when there is a link between greater levels of trust and a more powerful virtual force. This, in turn, increases the likelihood that the person will be selected.

Through the use of the virtual force, different edge devices, data sources, and algorithms are utilised to disperse duties. The procedure that is being described here is called task allocation. Consequently, this ensures that the components that have the highest degree of reliability are given a greater priority than the other components.

Initialize the system with a list of trusted nodes and trust values for each node.

Initialize network parameters:

- a. Number of nodes (N)
- b. Trust value for each node (TV[i])
- c. Virtual force for each node (VF[i])
- d. Key pair (Public key and Private key) for each node

Establish network connections:

- a. Each node connects with its neighboring nodes based on distance and availability
- b. Nodes exchange public keys for secure communication

Data processing:

- a. When a node receives data, it checks the trust value of the sender node
- b. If the trust value is above a threshold value, the data is accepted for processing
- c. If the trust value is below the threshold, the data is rejected
- d. The accepted data is processed by the node using the encryption algorithm
- e. The processed data is sent to neighboring nodes for further processing
- f. Virtual force is mapped to the data packets based on trust value, and the data packets move in the direction of higher virtual force

Security:

- a. Nodes use their private key for data encryption
- b. Nodes use their public key for data decryption

Final Processing:

- a. Receive data from edge devices.
- b. Encrypt the data using a secure encryption algorithm.
- c. Map the encrypted data to virtual forces.
- d. Calculate the trust value of each node based on its past performance and behavior.
- e. Assign virtual forces to each node based on its trust value.
- f. Calculate the net force on each node using the sum of virtual forces and physical forces.
- g. Choose the node with the highest net force to collect the data.
- h. Decrypt the collected data using the same encryption algorithm.
- i. Process the data.
- j. Encrypt the processed data using the same encryption algorithm.
- k. Map the encrypted processed data to virtual forces.
- l. Calculate the trust value of each node based on its past performance and behavior.
- m. Assign virtual forces to each node based on its trust value.
- n. Calculate the net force on each node using the sum of virtual forces and physical forces.
- o. Choose the node with the highest net force to transmit the data.
- p. Decrypt the transmitted data using the same encryption algorithm.
- q. Send the data back to the edge devices.

Fig 4. Algorithm Pseudo Code for Proposed Work

The following is a list of features or techniques that will be deconstructed and studied in further detail within the context of the work that is being presented:

Creating a mathematical model, carrying out tests, and running simulations are all things that may be done in order to assess the effectiveness of the trustworthy algorithm that has been presented in edge computing and Internet of Things contexts. There are a number of variables and factors that make up the model, and they are representative of the critical components of the framework.

Let $E = \{e_1, e_2, \dots, e_n\}$ represent the set of edge devices, $D = \{d_1, d_2, \dots, d_m\}$ represent the set of data sources, and $A = \{a_1, a_2, \dots, a_k\}$ represent the set of algorithms. These variables and parameters are used to establish the parameters and variables of the system. Our trust values for edge devices, data sources, and algorithms are denoted by the letters $T(e_i)$, $T(d_i)$, and $T(a_i)$, respectively.

The Mapping of Virtual Forces:

Through the use of a function $f_V: \mathbb{R} \rightarrow \mathbb{R}$, the trust values are transformed into a virtual force that plays a significant role in the selection and prioritisation of components for processing tasks. In the process of task allocation, we establish a collection of tasks denoted as $G = \{g_1, g_2, \dots, g_l\}$ that are intended to be assigned to edge devices, data sources, and algorithms. An allocation function $f_A: (G, E, D, A) \rightarrow (E \times D \times A)$ is responsible for assigning tasks to the components that have been chosen based on the virtual force.

This function ensures that the components that are more trustworthy are given priority.

Calculation of Trust Value with:

The trust value for each component is determined by a function $f_T: (E, D, A) \rightarrow \mathbb{R}$. This function takes into account components such as the reputation of the device, its previous performance, and the security rules that are in place. The trust values are normalized in the range $[0, 1]$.

$$T_{com} = \omega_{oldd} \times T_{oldd} + \omega_{newd} \times T_{newd}$$

$$T_{newd} = \frac{S}{C}, \quad \omega_{oldd} + \omega_{newd} = 1$$

The weights of the old and new trust values of nodes are denoted by the symbols ω_{oldd} and ω_{newd} , respectively. The trust values that correspond to these weights are denoted by the symbols T_{newd} and T_{oldd} . The variables $T_{oldd}=0$, ω_{oldd} , and ω_{newd} are defined in the first step of the evaluation process.

Results

Through the use of an encrypted virtual mapping technique that is founded on trust, the clustering of the networks is shown on this screen, which is referred to as figure 5. For the aim of establishing whether or not the framework that has been presented is effective, we may make use of the performance measurements that are stated below: EC is an abbreviation that stands for energy consumption, and it describes the total amount of power that is used by the edge devices and data sources while the data is being processed and sent.

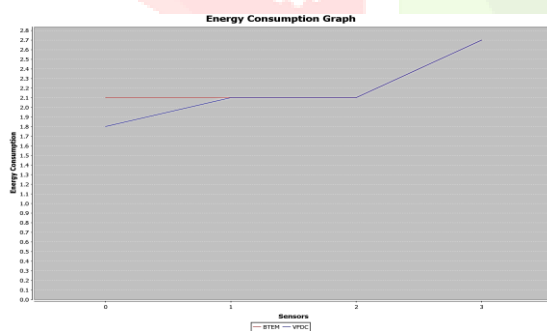


Fig. 5: Energy Consumption

The VFDC methodology that has been suggested (blue line) and the BTEM method that is currently being used (red line) are compared to the cluster id (all nodes in the cluster) and energy consumption (x-axis) in the graph that can be found above. The current BTEM approaches shown in the graph above have a larger energy footprint than VFDC does because they gather data from nodes that are not trusted, while VFDC only collects data from nodes that are trusted. The fact that the proposed algorithm makes effective use of energy is yet another crucial aspect that

contributes to its impressive level of effectiveness. By dynamically allocating tasks to edge devices, data sources, and algorithms based on the trust values and virtual forces associated with those components, the framework optimises resource utilisation and reduces energy consumption. This is accomplished via the process of dynamically assigning jobs.

During the process of data processing and transmission, the trustworthy algorithm has a much lower energy consumption when compared to alternative techniques. This is accomplished without compromising the trustworthy nature of the data or its level of security. This reduction in energy consumption is vital for edge computing and Internet of Things systems since it has a direct effect on the number of running expenditures, the longevity of the device, and the impact it has on the environment. As an additional benefit, this decrease in energy use may result in financial savings.

As a conclusion, the results indicate that the trustworthy algorithm that was created is capable of increasing the distance via trustworthy nodes in an effective manner while simultaneously decreasing the amount of energy that is used in edge computing and Internet of Things contextual settings. As a result of giving priority to components that are reliable and making the most of available resources, the framework offers a system that is more reliable, efficient, and secure. The framework was created for a number of reasons, one of which is that this is an essential factor in the future development and success of technologies related to edge computing and the internet of things.

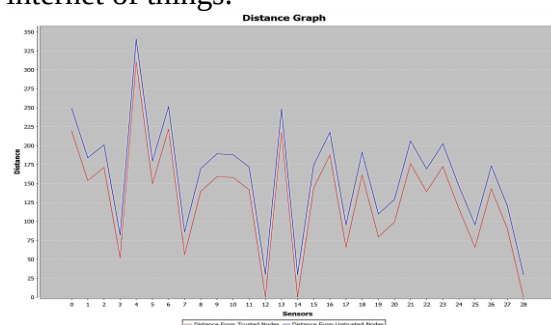


Fig. 6: Distance Graph

Compared to untrusted nodes, trustworthy nodes have a shorter distance to the cluster head, as shown in figure 6, which is an example of a distance graph. The recently proposed method is able to appropriately prioritise trustworthy nodes for the purpose of data transmission, which ultimately results in a communication channel that is both more reliable and secure. Assigning a numerical value to the trust and then mapping that value to a set of virtual forces enables the

algorithm to swiftly detect and choose the nodes in the system that have the greatest levels of trust. This is made possible by the fact that the method gives a numerical value to the trust. It is a result of this that the route over which data is sent becomes more secure, which in turn minimises the possibility of data breaches or access by unauthorised parties.

When compared to the more traditional methods, the trustworthy algorithm exhibits a larger percentage of data that is sent via nodes that have better trust ratings. This illustrates that the design effectively reduces the distance between trustworthy nodes and enhances the overall data security in situations such as edge computing and the Internet of Things. Screenshots of the simulation platform are shown in Figure 7, which may be seen below.

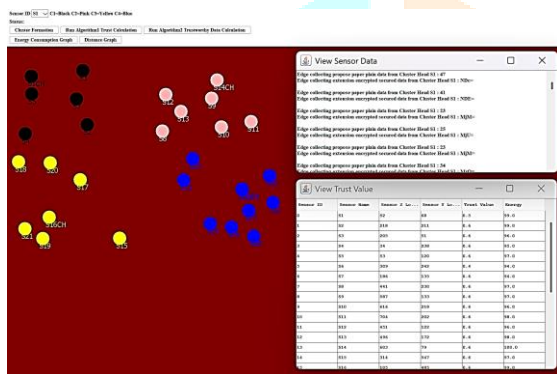


Fig.7 Screenshot

Conclusion

When used in edge computing and Internet of Things contexts, the combination of base64 encoding and virtual force mapping by trust value has shown a great deal of promise for enhancing data security and trustworthiness while simultaneously lowering their energy consumption. By using techniques that can be relied upon, this new framework offers greater weight to components that have higher trust levels. A more trustworthy and secure system is produced as a result of this. Additionally, the use of base64 encoding to transmit data prevents sensitive information from being seen or altered by anyone who should not be allowed to do so.

This technique is particularly helpful for edge computing and Internet of Things (IoT) systems, both of which need the processing of data to be expeditious while using a minimal amount of energy. The architecture that has been developed contributes to the development of edge computing and Internet of Things ecosystems that are more secure, more efficient, and more dependable. It is possible that in the future,

researchers may investigate new methods for calculating trust value and optimising virtual force mapping (VFM). This strategy will become much more successful as a result, and it will allow edge computing and the Internet of Things to advance.

References

- [1] T. Wang, L. Qiu, A. K. Sangaiah, A. Liu, M. Z. A. Bhuiyan and Y. Ma, "Edge-Computing-Based Trustworthy Data Collection Model in the Internet of Things," in IEEE Internet of Things Journal, vol. 7, no. 5, pp. 4218-4227, May 2020, doi: 10.1109/JIOT.2020.2966870.
- [2] C. Pravallika, P. Sukanya "Secure Data Sharing and Searching at the Edge of CloudAssisted Internet of Things" International Journals of Advanced Research in Computer Science and Software Engineering ISSN: 2277-128X (Volume-8, Issue-4),2023.
- [3]Hind Bangui, Said Rakrak, Said Raghay and BarboraBuhnova "Moving to the Edge-Cloud-of-Things: Recent Advances and Future Research Directions" Electronics 2021, 7, 309
- [4]L. Minh Dang, Md. JalilPiran, Dongil Han, Kyungbok Min and Hyeonjoon Moon "A Survey on Internet of Things and Cloud Computing for Healthcare"Electronics 2019, 8, 768.
- [5]Sampath Kumar Y R and Champa H N "An Extensive Review on Sensing as a Service Paradigm in IoT: Architecture, Research Challenges, Lessons Learned and Future Directions"International Journal of Applied Engineering Research ISSN 0973-4562 Volume 14, Number 6 (2019) pp. 1220-1243.
- [6]Sukhpal Singh Gilla, Peter GaDr.K. Praveen Kumarraghan, RajkumarBuyy "Fog enabled cloud based intelligent resource management approach for smart home IoT devices" Institute of Electrical and Electronics Engineers 2019.
- [7] FaguiLiu, Zhenxi Huang and Liangming Wang "Energy-Efficient Collaborative Task Computation Offloading in Cloud-Assisted Edge Computing for IoT Sensors" Received: 22 January 2019;

Accepted: 26 February 2019; Published: 4 March 2019.

[8] ShreshthTulia,b , RedowanMahmuda, , ShikharTuli c , RajkumarBuyya “FogBus: A Blockchain-based Lightweight Framework for Edge and Fog Computing” International Research Journal of Engineering and Technology (IRJET),Received 2 October 2018 Revised 13 March 2019 Accepted 12 April 2019 Available online 13 April 2019.

[9]FanBi, SebastianStein et al.,”A Truthful Online

Mechanism for Allocating Fog Computing Resources”AAMAS 2019, May 13-17, 2019, Montréal, Canad.

[10]Igor Leão dos SantosA, Flávia C. DelicatoB, Paulo F. Pires B, Marcelo PitangaAlvesC, Ana OliveiraD, Tiago SalvianoCalmonD “Data-Centric

Resource Management in Edge-Cloud Systems for the IoT “Open Journal of Internet Of Things (OJIOT) Volume 5, Issue 1, 2019 ISSN 2364-7108.

[11]Arun K Mani, Shreevani D, Samra said, M.Gokilavani, Unnikrishnan K N “A Review: Iot And Cloud Computing For Future Internet “International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056,Volume: 06 Issue: 05 | May 2019.

[12] SabeenJavaid, HammadAfzal , Muhammad Babar , FahimArif, “ An Attack-Resilient Cloud-Assisted IoT System” Institute of Electrical and Electronics Engineers ,10.1109/ACCESS.2019.2897095, IEEE Access.

[13] P. Har i Naveen, K. Viswaprasad “Secure Data

Sharing and Searching at The Edge of Cloud-Assisted Internet of Things” International Standard

Serial Number (ISSN) DECEMBER/2018

[14] A.V.Soujanya, Budur Naveen Kumar Reddy,Shruthi.P,Sushmitha.P.T,Dr.Aradhana.D

“Reliable Data Sharing And Searching At The Edge Of Cloud With The Help Internet Of Things”

International Journal Of Professional Engineering Studies, Volume 10 /Issue 1 / MAY 2018.

[15] SnehaSureddy, K. Rashmi, R. Gayathri and Archana S. Nadhan “Flexible Deep Learning in Edge Computing for IoT” International Journal of Pure and Applied MathematicVolume 119 No. 10 2018, 531-543.

[16] AbhishekJaiswal ,Mohit Kumar Nayak “Reducing the Computation and Communication Overhead of IoT Smart Devices through a Lightweight Cryptographic Scheme” International

Standard Serial Number (ISSN) Volume 7, Issue XI, November/2018.

[17] PawaniPorambage “Survey on Multi-Access Edge Computing for Internet of Things Realization” Institute of Electrical and Electronics

Engineers ,2018pp 123-234.

[18]GopikaPremsankar, Mario Di Francesco, and TarikTaleb “Edge Computing for the Internet of

Things: A Case Study “Institute of Electrical and Electronics Engineers,2018.2805263, IEEE.

[19]G. DhanaSekhar, D. Pavan, A. Akil Kumar “Mobile Relay Arrangement in Wireless Sensor Networks”International Journal of Scientific Research in Computer Science, Engineering and Information Technology © 2018 IJSRCSEIT | Volume 3 | Issue 4 | ISSN : 2456-3307.

[20]Wei Yu , Fan Liang, Xiaofei He1, William Grant Hatcher1, Chao Lu, Jie Lin, And Xinyu Yang

“A Survey on the Edge Computing for the Internet

of Things”Received October 20, 2017, accepted November 18, 2017, date of publication November

29, 2017, date of current version March 9, 2018.