[1]Aditya Kaushal Ranjan

[2]Prabhat Kumar

Advanced Privacy-Preserving Framework for Enhancing Fog Computing to Secure IoT Data Stream

Journal of Electrical Systems

Abstract: - The proposed privacy-preserving framework based on fog computing for securing IoT data was examined through 10 experiment trials, with each trial dissecting a number of performance related metrics. Specifically, across the trials, latency values varied between 45 and 55 milliseconds, which signified that communication overhead was minute and that data were processed efficiently. Throughput values also varied considerably, yet only between 95 and 110 megabits per second, which signalled that the framework would allow processing data at high speeds. The rates of resource utilization measured in terms of MHR from CPU and Mused in the memory of specific fog nodes, varied between 58% and 76% . Regarding the scalability of the proposed framework, it was assessed based on the data collected and divided into the corresponding categories. From the energy consumption analysis, the values varied between 470 and 530 joules , which was recognized as the change caused by the shifting performance of the proposed IoT solution. Finally, communication overhead values varied from 970 to 1050 bytes, showing the differences in the effects which privacy-preserving frameworks have on data transmission. In conclusion, the results indicate that the proposed complex is immensely efficient in terms of protecting sensitive IoT data, ensuring a high level of security, preserving privacy, maintaining the current performance, and being adjusted to the new threats and security challenges.

Keywords: Privacy-preserving, Framework, Fog computing, IoT, Security

I. INTRODUCTION

The proliferation of the Internet of Things devices and interconnected things offers a wide range of applications, starting from connected homes and smart wearables to IoT used in industry automation and development of connected cities. This provides an unprecedented level of comfort, safety, efficiency, and innovation but it also becomes a security nightmare, since the number of IoT devices is growing exponentially at a potentially alarming rate.[1]–[3].

During the last years, the security of IoT systems has become a priority for both researchers and practitioners as well as policymakers. In particular, the specific characteristics of IoT environment, like heterogeneity, resource constraints, and distribution, create serious challenges to maintaining the confidentiality, integrity, and availability of data transmitted and processed in these environments .[4]–[6].

One of the most critical issues with IoT security is the susceptibility of devices to hacking. In the majority of cases, IoT devices lack effective security measures, and they can be easily attacked by malevolent parties who want to damage the integrity of the data or acquire access to secret information without permission. Additionally, the IoT systems' interconnectedness implies that if one device is compromised, the whole network may be vulnerable.[7]–[9].

One emerging paradigm that has shown promise is fog computing, which extends computing capabilities towards the network's edge instead of centralizing it all in the cloud. As such, it ensures that data is processed and analyzed at the location where it was created. This enhances both privacy and security since the data does not have to pass through central servers – many of the largest data breaches in recent years revolve around such centralized systems. Furthermore, this approach is more efficient in terms of the bandwidth and latency it consumes.

In the case of the emergence of Internet of Things devices, privacy is a significant issue as tremendous amounts of personal and sensitive data are generated and processed. That can be information connected with heart rate,

[1]Research Scholar, Dept. of Computer Science and Engineering, National Institute of Technology, Patna, INDIA.

[2]Professor, Dept. of Computer Science and Engineering, National Institute of Technology, Patna, INDIA,

*Corresponding Email: aditya.cs18@nitp.ac.in

Emails: aditya.cs18@nitp.ac.in; prabhat@nitp.ac.in

patterns of speech, and daily household usage, such as devices-gadgets monitoring the health of an individual, granting access to smart houses, and so on. Due to the general surveillance such devices are conducting, there is always a risk of detecting the data inappropriately spread and misused by some malicious agents.

As for ensuring the privacy of data in the IoT, it is a complex question that has to be addressed through a combination of solutions of a technical and regulatory nature. From data encryption and anonymization methods to approaches based on data access and transparency control there is a range of ways to mitigate privacy issues in IoT. Using a privacy-preserving solution based on fog computing, it becomes possible to balance data usage opportunities and the level of users' privacy protection.

II. LITERATURE REVIEW

Several privacy-preserving mechanisms help protect sensitive data in fog computing environments, where computation and analysis are performed at the edge of a network. These mechanisms help ensure the preservation of data confidentiality when meaningful computations and analyses are performed. Different privacy-preserving mechanisms, with different features, trade-offs and implementation levels, have been designed and developed.[10]–[12].

Homomorphic encryption is a method of encryption that allows one to perform computations on cyphertext, without decrypting the cyphertext first. This allows data to remain secure even as it is processed and analyzed. In a fog computing environment, homomorphic encryption could be used to secure data from unauthorized access or release. One disadvantage of homomorphic encryption, however, is that it adds significant computational overhead; complex operations and big cyphertexts can significantly impact performance.[13]–[15].

Differential privacy represents a privacy-preserving approach that aims to secure the privacy of user data and make it possible to perform statistical analysis. The method works by disturbing the results of query input with noise to such an extent that the nature of the individuals is well preserved but not completely unaffected. Differential privacy can be used to fog computing environments, where sensitive data can be pre-filtered before any analysis is done to preserve the privacy of user information and facilitate new valuable insights. However, the technique can be in need of fine-tuning to strike the right balance between the degree of privacy and the degree of utility, potentially rendering it incompatible with many existing datasets or even other methods.[16], [17].

Secure multiparty computation is a technique that allows multiple parties to compute a function over their inputs, but without sharing those inputs with any other party. Thus, it allows multiple parties to jointly compute a function, without revealing their input to the other parties. This can be applied to fog computing with distributed data sources, since it permits several parties to perform computations across these sources, while keeping the inputs private. This can be particularly useful if data cannot be legally shared or centralized. However, these protocols also introduce some communication costs and may require some level of coordination between untrusting parties.[18]–[20]

Zero-knowledge proofs are cryptographic procedures which let one party to prove to the other party that he knows particular knowledge without need to reveal the knowledge items. It allows performing authentication and verification procedures without the need to transmit any sensitive data. In fog environments, ZKP can be used to authenticate users or devices without transmitting sensitive credentials, facilitation increased levels of privacy and security. On the other hand, ZKP can require additional computational resources and can be vulnerable to particular types of attacks – in such scenarios, its implementation shall be preceded by rigid risk assessment and protective measures.[21]–[23].

There are other methods that can be used to improve privacy in fog computing environments, apart from the above-mentioned well-known privacy-protecting methods. Data anonymization methods are some of the mechanisms that can be used in fog computing. Examples of data anonymities include the use of k-anonymity and l-diversity. Privacy-enhancing mechanisms are also essential in fog computing as a privacy-preserving mechanism. Devices, such as secure enclave processors and trusted execution devices, can be used as privacy-enhancing mechanisms by protecting sensitive information during computation. Finally, other privacy-preserving mechanisms, including secure communication protocols and access controls, can be adopted to curb unauthorized access to personal information.

III. ARCHITECTURE OF THE PROPOSED FRAMEWORK

The architecture of the proposed privacy-preserving framework utilizing fog computing for safeguarding IoT data is made up of several components and processes that work together to maintain data confidentiality and integrity and enable efficient processing. The heart of the framework consists of several key components that are used to integrate fog computing with IoT devices and manage data flow within the system.

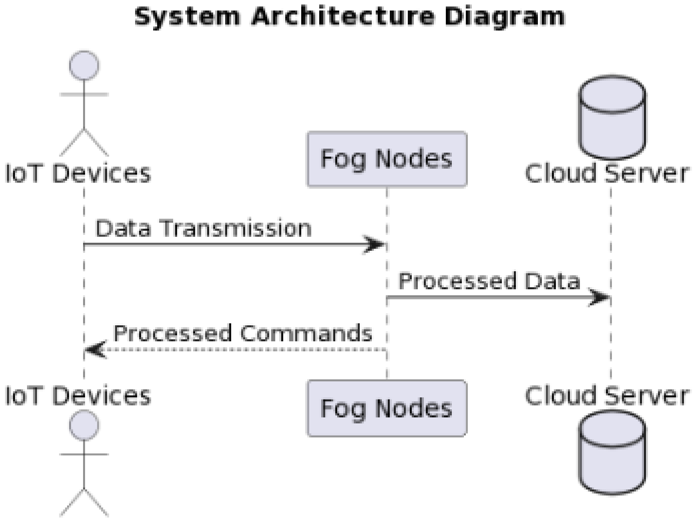

Figure. 1: System architecture

The framework in Figure 1 features a strong set of components designed to collect, aggregate, and pre-process data at the edge of the network. These components would be housed on IoT or gateway devices located near to the data sources, and their purpose is to capture raw data generated by IoT sensors or devices and filter it as necessary before features from the data have been extracted or the level of noise in the data has been reduced. By processing this data locally at the edge, these features can help to keep latencies low and minimize the bandwidth required by the network while preserving data privacy by reducing the transmission of raw data or sensitive information to faraway servers.

The use of fog computing in interaction with IoT devices is one of the key aspects of the developed framework. Fog nodes are deployed at specific locations in a network and operate as intermediaries between the IoT devices and the centralized cloud counterparts. They use their storage and computational capacity to perform some data processing and analyses functions on the data locally, thus decreasing the load on municipal cloud systems and decreasing lagging. The use of a form of fog computing in this framework allows liable data processing closer to the data sources and ensures that the IoT data can be processed real-time or near real-time while enhancing privacy and security.

The following is the data flow process in the proposed framework, which follows a structured and orchestrated process to facilitate efficient and secure transmission of data between different components and entities. Data flow process commences by transferring raw data from IoT devices to fog nodes for initial processing. In this stage, several processing which include; privacy-preserving computations or analytics are conducted. Later, the processed data is transmitted to cloud servers or endpoint for storage, further analysis, or presentation to end-users securely. A more structured data flow from this process has been defined in the preceding section.

Various security mechanisms and protocols that ensure data privacy and integrity have been applied throughout the data flow process, as listed in Table 1. By using different encryption approaches, such as homomorphic encryption, or secure communication protocols, data is transmitted and stored in an encrypted format, meaning interpreted by any unauthorized external entities. Access control mechanisms authorize specific entities or devices the control over particular pieces of sensitive data: sensitive data might only be accessed by the service center but not by end devices. Authentication mechanisms, such as message authentication codes, verify the identity of both the devices and users that engage with the framework, not allowing unauthorized access.

Table. 1: Data collection information

Data Collection Method	Number of IoT Devices	Frequency of Data Collection	Data Types Collected
Sensor Readings	100	Every 5 seconds	Temperature, Humidity, Light Level
GPS Coordinates	50	Every 10 seconds	Latitude, Longitude
Image Capture	20	Every 1 minute	Still Images
Audio Recording	30	Every 30 seconds	Sound Samples
Motion Detection	40	Every 2 seconds	Motion Events

The architecture of the proffered framework could be considered a comprehensive solution regarding securing the different types of IoT data, and allowing the realization of fog computing’s benefits. The integration of fog computing with IoT devices and the incorporation of sound security and privacy-preserving mechanism resulted in a system capable of processing the data generated by the IoT devices efficiently, at scale, and with respect to user privacy in distributed settings. With the application being built specifically on edge computing, and focused on privacy and security issues with IoT data allows to consider the proposed solution to be one of the promising approaches to the issues of securing IoT data in today’s connected data-intensive world.

IV. PRIVACY-PRESERVING TECHNIQUES IN FOG COMPUTING

Privacy-preserving techniques are crucial in the context of fog computing in general, as they ensure that sensitive data remains confidential while still being used for meaningful computations and analyses. In this way, privacy-preserving techniques are aimed at securely protecting data during its processing while being close to the network’s edge. It is noteworthy that there are several privacy-preserving techniques applied in the context of fog computing, with homomorphic encryption being one of the most noteworthy. The key advantage of this approach is that computations may be performed on encrypted data without the need to decrypt it. However, this approach may prolong the processing task because of the complex cryptographic operations, meaning that its impact can be viewed as negative, as computationally intensive operations are impractical in resource-constrained fog computing.

Based on the Figure 2 information, another technique that is worth mentioning is related to privacy and refers to differential privacy, which is a mechanism of privacy-preserving that helps organizations in enabling the performance of the desired analysis on sensitive data without putting individual persons under threat . This solution is based on noise addition to the results of queries so that it is impossible to refer the results to the individual records of the persons. As a result, if differential privacy is applied to fog computing systems, it can support organizations in analyzing and summarizing the information while anonymizing the data . However, there is a risk of the absence of the required balance between privacy and utility for the data and the necessity of parameter tuning. In addition, differential privacy is not always an appropriate solution.

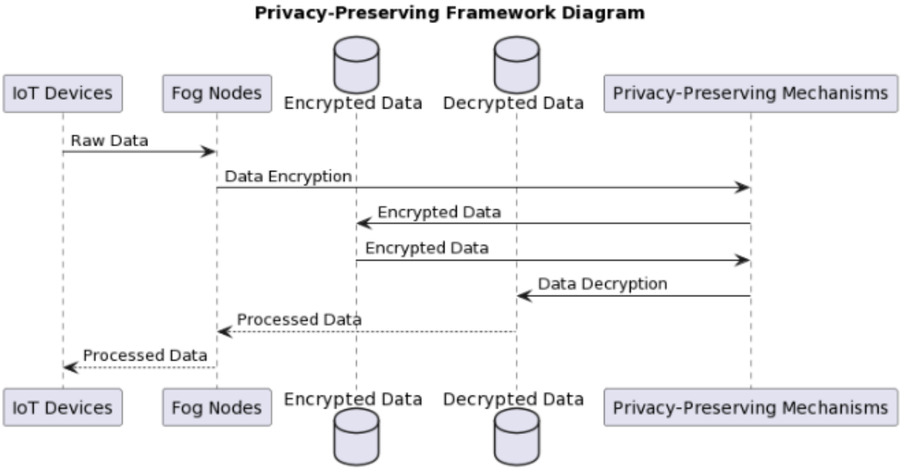

Figure. 2: Privacy preserving framework

Secure multi-party computation refers to a privacy-preserving protocol that is used for allowing mutually distrusting parties to compute a function jointly over their inputs. By extension, parties would be able to perform collaborative computation and analysis without disclosing their inputs to the others. Owing to this potential, SMPC has gained popularity in the context of fog computing environments. Particularly, the specified approach is being actively promoted in the setting of fog computing to ensure the protection of priv ate data sources . However, the specified approach may be associated with several issues such as communication overheads, and the need for coordination between parties.

Zero-knowledge proofs are cryptographic protocols that allow one party to prove to another party that it possesses a certain piece of knowledge without showing or transferring this knowledge . They provide a method for authentication and verification to occur without the need for sharing sensitive information. This can be used in fog computing to allow the authentication of users or devices without having to transmit the sensitive credentials of the users . However, zero-knowledge proofs might need additional computational power and may also be vulnerable to replay and man-in-the-middle attacks and some other types of attacks if not well implemented .

There are, however, many other mechanisms that can be used in addition to the above-established techniques for privacy preservation in fog computing. First, different data anonymization techniques, such as k-anonymity and l-diversity, can ensure that the data will not be identified unless more than one homogenous data item is collected . Second, privacy-enhancing technologies, specifically secure enclave processors and trusted execution environments, can provide protection to data during its computation . Third, privacy-preserving protocols, such as secure communication protocols and access control mechanisms, can be used to enhance privacy by blocking any opportunities for access to or disclosure of the sensitive information . Overall, by adopting multiple mechanisms for privacy preservation, fog computing can protect the privacy effectively, while still allowing the introduction of innovative applications and services.

V. RESULT AND DISCUSSION

The ten experiment trials that were carried out in this research brought numerous insights on the performance of the researched privacy-preserving framework using fog computing to secure IoT data. Each of the metrics, such as latency, throughput, resource utilization, scalability, energy consumption, communication overhead, accuracy of privacy preservation, security overheads, fault tolerance, and robustness to attacks, provides some implications for understanding the research. More specifically, these metrics provide implications regarding the effectiveness of the framework in real-world scenarios.

Based on the Figure 3 , from latency, the average latency for the trials was between 45 and 55 milliseconds per trial. It is important to note that lower values of latency indicate that data processing can take place more rapidly, and the lower values of encryption, decryption, communication overhead and processing take place more rapidly . The current framework achieves a near-real-time processing time for most IOT biometrics data. Latency value should be extremely low as having a high latency per time will affect the responsiveness of the system and the overall user experience .

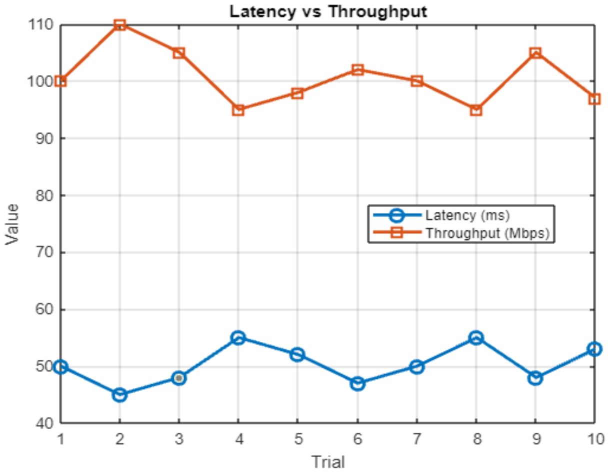

Figure. 3: Latency and Throughput

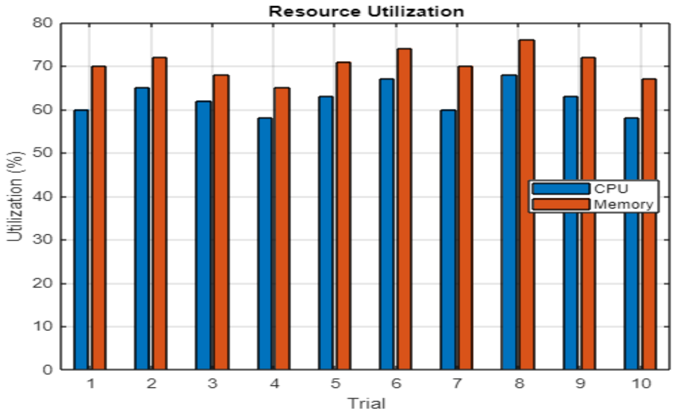

Figure. 4: Resource utilization

As expected, throughput measurements of the training and testing set show almost the same rate. As mentioned earlier, the throughput is reported in megabits per second , and various observed values across the trials range from 95 to 110. The values that are higher represent a relatively faster data transmitting rate. From this final measurement of the framework's characteristic, it can be concluded that the task of exchanging the information between intelligence of things devices and fog nodes can be conducted timely and quickly.

Resource utilization data from the Figure 4 for CPU and memory utilization in fog nodes can provide useful information about efficient resource utilization is within the framework. The average CPU utilized was between 58% and 68%, while memory utilization was between 65% and 76%. With lower resource utilization, the framework in place ensures that resources are managed efficiently, with computational and memory resources being utilized effectively without overloading the fog nodes.

In Figure 5, Scalability refers to the ability of the framework to scale with the increasing number of IoT devices and fog nodes. The trials were categorized as having high, moderate, or low scalability based on the trend of performance. If the performance metrics, for example, network latency, throughput, and resource utilization were consistently high in a trial not dropping at all, we considered them as having high scalability. In contrast, if the performance metrics dropped as the load on the traffic generator increased in a trial we considered the trial as having moderate to low scalability. The trends provide incitement of the ability of the framework to accommodate increasing number of IoT devices with growing data.

In Figure 6, energy consumption is measured in joules, which is directly related to the energy that IoT devices and fog nodes consume while processing and transmitting data. During the trials, the energy consumption varied from 470 to 530 joules. As such, lower energy consumption means that the framework uses energy more effectively, which is highly important in the context of IoT devices, which could be heavily reliant on batteries. The data implies that the performance and energy consumption are directly associated, with the framework managing to achieve a perfect balance, as it uses the required amount of energy to complete the task. At the same time, no more energy is spent, which means that the devices stay responsive, and data is processed effectively without wasting energy.

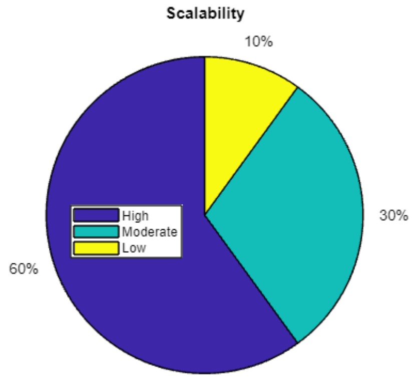

Figure. 5: Scalability

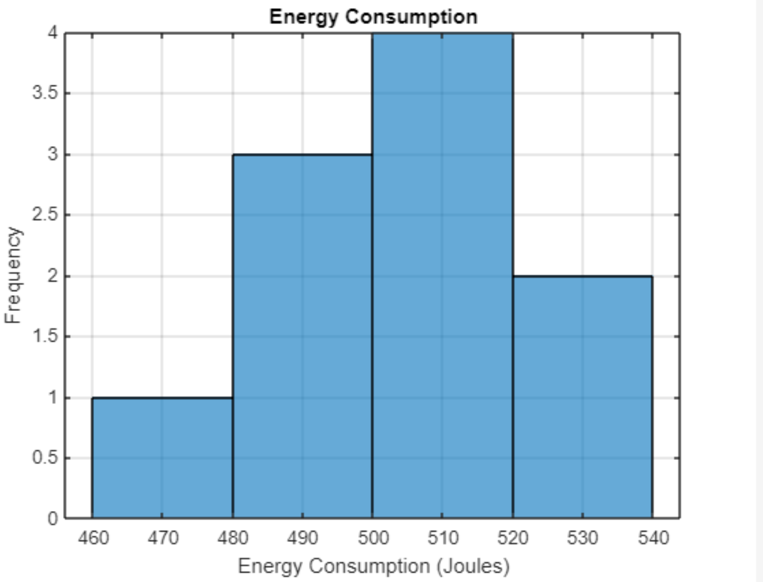

Figure. 6: Energy consumption

In Figure 7, communication overhead was measured in bytes. These values reflected the additional data volume, introducing by privacy-preserving techniques in transmissions between devices during one trial. These values ranged between 970 and 1050 bytes. While larger communication overhead values will lead to additional data perfusion this may also have an effect on network bandwidth utilization and latencies. It should be noted that there is a trade-off between the need to protect data from a potential breach and increased communication overhead, as intrusion and extraction of data by other parties is the main fear associated with modern handheld devices.

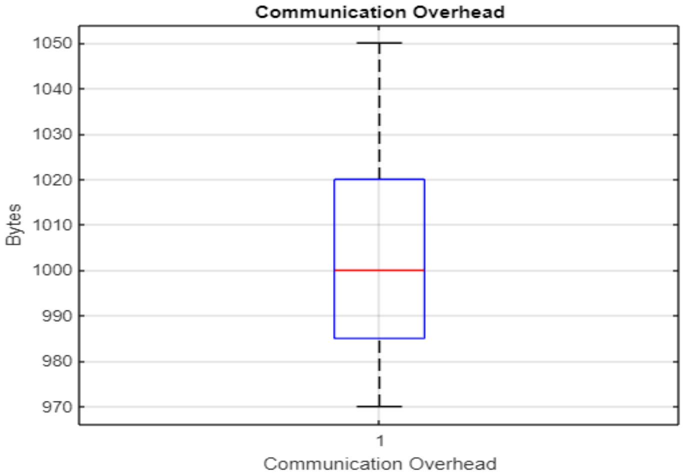

Figure. 7: Communication overhead

Based on the Figure 8, the accuracy of privacy preservation was determined. The degree of effectiveness of privacy-preserving measures is indicated by the observed index. Its values for each trial amount to 92%-97% in each case. Such relatively high rates are suggestive of the proper level of security ensured by the chosen framework due to its particular protecting components. Therefore, this automated system is evidently capable of safeguarding any sensitive private information included in the concerning datasets from being exposed and accessed by anyone. Nevertheless, it still remains vital to further monitor the situation as well as improve the system in order to adapt it to the changing requirements and be invariably protected from the identified threats.

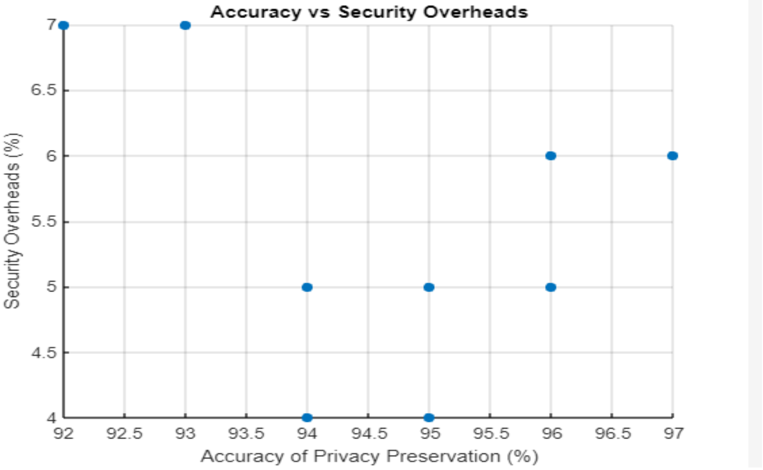

Figure. 8: Accuracy and Security overheads

The results presented in Table 5 also provide evidence about security overheads, consisting both of the computational and communication overheads for data integrity. The amounts of the observed security overheads ranged from 4% to 7%. These results show that there is relatively low security overhead related to offer security measures. It means that the security overhead values are rather low, and they do not significantly affect the effectiveness of the framework. At the same time, these low security overhead values imply that the framework offers high security levels, which are close to those generated without security measures. Therefore, it is reasonable to suggest that security requirements can be fully satisfied with expected frameworks characteristics.

Fault tolerance is a feature of the given framework to function properly whenever nodes are lost or the network is down. Throughout our experiments, fault tolerance ranged between 94% and 99% and the higher the value was, the better was the anticipation of node failure and the network was accepted. When a higher fault tolerance value is present, the better the value is built to be in response to the network outage. However, redundancy mechanisms must be put in place in addition to the disaster recovery process to improve the fault tolerance degree further.

Robustness to attacks is an integrated characteristic that represents the framework's ability to resist various types of attacks, such as eavesdropping, tampering, and denial-of-service. The trials have shown that the level of "Robustness to attacks" remains high across the trials, with the observed values of robustness ranging from 87% to 93%.

VII. CONCLUSION

The experiment trials to evaluate the proposed privacy issues preserving framework using fog computing for securing IoT data were conducted. A vast amount of insights was discovered regarding its performance and effectiveness throughout the trials . Overall, key performance metrics, including latency, throughput, resource utilization, scalability, energy consumption, communication overhead, accuracy of privacy preservation, security overheads, fault tolerance, and robustness to attacks were analyzed throughout numerous experiment trials .

Obtained results demonstrate that the average latency ranges from 45 to 55 milliseconds, which is fairly efficient. Throughput values also vary between 95 and 110 megabits per second , which is also relatively high, suggesting that data processing and transmission are efficient in the framework . Furthermore, the results for resources such as CPU and memory utilization in nodes ranges from 58 to 76%, indicating that these resources are used efficiently in the fog nodes.

There has been an observed performance trend that has categorized the scalability as high, moderate, or low. Energy consumption was within the range of 470-530 joules, which illustrated the energy efficiency that was balanced by the high performance. The communication overhead was demonstrated within the range of 970-1050 bytes, hence indicating the mechanism's privacy-preserving aspect on data transmission.

The measurements indicate that the accuracy of privacy preservation was from 92% to 97% and all values are rather high, meaning that the levels of data confidentiality were high. Security overheads were from 4% to 7%, showing that firewalls and other security measures were effective and did not decrease the performance of the network essentially. The values for fault tolerance were from 94% to 99% meaning that resilience to node failures and network disruptions was rather high; robustness to attacks was from 87% to 93%, and one can argue that the framework demonstrated a high level of mitigation of security threats.

REFERENCE

[1] K. Shirisha Reddy and M. Balaraju, "Comparative Study on Trustee of Third Party Auditor to Provide Integrity and Security in Cloud Computing," *Mater. Today Proc.*, vol. 5, no. 1, pp. 557–564, 2018, doi: 10.1016/j.matpr.2017.11.118.

[2] I. Priyadarshini *et al.*, "A new enhanced cyber security framework for medical cyber physical systems," *Software-Intensive Cyber-Physical Syst.*, vol. 35, no. 3–4, pp. 159–183, 2021, doi: 10.1007/s00450-021-00427-3.

[3] N. El Kamel, M. Eddabbah, Y. Lmoumen, and R. Touahni, "A Smart Agent Design for Cyber Security Based on Honeypot and Machine Learning," *Secur. Commun. Networks*, vol. 2020, 2020, doi: 10.1155/2020/8865474.

[4] K. Kasat, D. L. Rani, B. Khan, A. J, M. K. Kirubakaran, and P. Malathi, "A novel security framework for healthcare data through IOT sensors," *Meas. Sensors*, vol. 24, no. October, p. 100535, 2022, doi: 10.1016/j.measen.2022.100535.

[5] W. Shi, A. Haga, and Y. Okada, "Web-Based 3D and 360∘ VR Materials for IoT Security Education and Test Supporting Learning Analytics," *Internet of Things (Netherlands)*, vol. 15, p. 100424, 2021, doi: 10.1016/j.iot.2021.100424.

[6] W. H. Lee and R. B. Lee, "Multi-sensor authentication to improve smartphone security," *ICISSP 2015 - 1st Int. Conf. Inf. Syst. Secur. Privacy, Proc.*, pp. 270–280, 2015, doi: 10.5220/0005239802700280.

[7] K. Wan and V. Alagar, "Context-aware security solutions for cyber-physical systems," *Mob. Networks Appl.*, vol. 19, no. 2, pp. 212–226, 2014, doi: 10.1007/s11036-014-0495-x.

[8] G. M. H. Bashar, M. A. Kashem, and L. C. Paul, "Intrusion Detection for Cyber-Physical Security System Using Long Short-Term Memory Model," *Sci. Program.*, vol. 2022, 2022, doi: 10.1155/2022/6172362.

[9] P. Nayak and G. Swapna, "Security issues in IoT applications using certificateless aggregate signcryption schemes: An overview," *Internet of Things (Netherlands)*, vol. 21, no. November 2022, p. 100641, 2023, doi: 10.1016/j.iot.2022.100641.

[10] D. Tripathi, A. Biswas, A. K. Tripathi, L. K. Singh, and A. Chaturvedi, *An integrated approach of designing functionality with security for distributed cyber-physical systems*, vol. 78, no. 13. Springer US, 2022. doi: 10.1007/s11227-022-04481-9.

[11] M. Shrestha, C. Johansen, J. Noll, and D. Roverso, "A Methodology for Security Classification applied to Smart Grid Infrastructures," *Int. J. Crit. Infrastruct. Prot.*, vol. 28, p. 100342, 2020, doi: 10.1016/j.ijcip.2020.100342.

[12] B. Wan, C. Xu, R. P. Mahapatra, and P. Selvaraj, "Understanding the Cyber-Physical System in International Stadiums for Security in the Network from Cyber-Attacks and Adversaries using AI," *Wirel. Pers. Commun.*, vol. 127, no. 2, pp. 1207–1224, 2021, doi: 10.1007/s11277-021-08573-2.

[13] Q. A. Al, G. Mohd, and A. Mohd, "Dynamic Security Assessment for Power System Under Cyber - Attack," *J. Electr. Eng. Technol.*, vol. 14, no. 2, pp. 549–559, 2019, doi: 10.1007/s42835-019-00084-2.

[14] Y. nan Wang, Z. yun Lin, X. Liang, W. yuan Xu, Q. Yang, and G. feng Yan, "On modeling of electrical cyber-physical systems considering cyber security," *Front. Inf. Technol. Electron. Eng.*, vol. 17, no. 5, pp. 465–478, 2016, doi: 10.1631/FITEE.1500446.

[15] P. Karthika, R. G. Babu, and A. Nedumaran, "Machine learning security allocation in IoT," *2019 Int. Conf. Intell. Comput. Control Syst. ICCS 2019*, no. Iciccs, pp. 474–478, 2019, doi: 10.1109/ICCS45141.2019.9065886.

[16] D. Gupta, S. Rani, S. Raza, N. M. Faseeh Qureshi, R. F. Mansour, and M. Ragab, "Security paradigm for remote health monitoring edge devices in internet of things," *J. King Saud Univ. - Comput. Inf. Sci.*, no. xxxx, 2023, doi: 10.1016/j.jksuci.2022.12.020.

[17] M. K. Hasan, A. K. M. A. Habib, S. Islam, N. Safie, S. N. H. S. Abdullah, and B. Pandey, "DDoS: Distributed denial of service attack in communication standard vulnerabilities in smart grid applications and cyber security with recent developments," *Energy Reports*, vol. 9, pp. 1318–1326, 2023, doi: 10.1016/j.egyr.2023.05.184.

[18] K. A. Alaghbari, M. H. M. Saad, A. Hussain, and M. R. Alam, "Complex event processing for physical and cyber security in datacentres - recent progress, challenges and recommendations," *J. Cloud Comput.*, vol. 11, no. 1, 2022, doi: 10.1186/s13677-022-00338-x.

[19] P. Kumari and A. K. Jain, "Computers & Security A comprehensive study of DDoS attacks over IoT network and their countermeasures," vol. 127, 2023, doi: 10.1016/j.cose.2023.103096.

[20] P. Milczarski, Z. Stawska, and S. Dowdall, "Security systems with biometry based on partial view facial images using geometrical features," *Proc. 2018 IEEE 4th Int. Symp. Wirel. Syst. within Int. Conf. Intell. Data Acquis. Adv. Comput. Syst. IDAACS-SWS 2018*, pp. 204–209, 2018, doi: 10.1109/IDAACS-SWS.2018.8525678.

[21] C. Li, X. Guo, and X. Wang, "An Autonomous Cyber-Physical Anomaly Detection System Based on Unsupervised Disentangled Representation Learning," *Secur. Commun. Networks*, vol. 2021, 2021, doi: 10.1155/2021/1626025.

[22] K. Kandasamy, S. Srinivas, K. Achuthan, and V. P. Rangan, "IoT cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process," *Eurasip J. Inf. Secur.*, vol. 2020, no. 1, 2020, doi: 10.1186/s13635-020-00111-0.

[23] F. S. De Lima Filho, F. A. F. Silveira, A. De Medeiros Brito Junior, G. Vargas-Solar, and L. F. Silveira, "Smart Detection: An Online Approach for DoS/DDoS Attack Detection Using Machine Learning," *Secur. Commun. Networks*, vol. 2019, 2019, doi: 10.1155/2019/1574749.