Pioneering Security: A Hybrid Logic Framework for the Future of IoT Protection

Rajeev Shrivastava
Principal, Princeton Institute of Engineering & Technology for Women Hyderabad, Telangana, India
Emails: rajeev2440130@gmail.com; principal@petw.in

Abstract

In a complicated situation, the Internet of Things simplifies the process of connecting a wide range of things. Because of its openness and lack of human control, the Internet of Things is open to assaults like denial of service (DoS) and man-in-the-middle attacks. Furthermore, any device that can connect to the internet may be hacked. These attacks put the network connections and the actual equipment at danger. IoT security and privacy will so be compromised. Due to its limited power, bandwidth, and storage, the Internet of Things requires a security solution that does not overload it. This study aims to preserve consumers' trust in the Internet of Things (IoT) by safeguarding their data against unauthorised access and maintaining the privacy of their personal information. With the ultimate objective of presenting a unique hybrid and optimised lightweight logical security architecture to ensure data privacy and integrity while making effective use of available resources, all research are carried out with this purpose in mind. The Hybrid Lightweight Security Framework (HLSF), which this study suggests, offers secrecy and integrity in addition to authentication. The structure consists of three distinct steps. The first step is registration, the second is authentication, and the third is transit security, which protects data while it is being transported. Compared to other current frameworks, the results reveal that HLSF performs better in terms of precision, recall, and accuracy when applied to an IoT situation.

Keywords: IoT; HLSF; COAP; Security.

1. Introduction:

Now-a-days There will be new opportunities for invasions of privacy and threats to security as a result of the Internet of Things' introduction into residential and commercial settings. As a result, concerns over security and privacy in IoT operations are growing. If an assault were to be inserted into the IoT, the potential loss is staggering [1]. Many different types of assaults can be launched against the Internet of Things. These attacks will compromise the privacy of users and undermine IoT security services like confidentiality, integrity, and authentication. At each stage, the IoT's built-in basic security solutions are open to attacks [2].

Due to limitations in the IoT situation, such as electricity and real-time execution, traditional cryptography and authentication systems are not a good fit. As a result, IoT is best served by lightweight cryptographic methods. The Internet of Things (IoT) is a next-generation technological breakthrough in the realm of intelligent machines. The Internet of Things aims to supply services for application development, including data collecting, data management, and data and device security [3]. In IoT, objects or gadgets exchange data and do computations to improve our quality of life and security. The Internet of Things (IoT) allows for real-time inventory checks, item information management, status monitoring, and monitoring.

Doi : https://doi.org/10.54216/JCIM.130104
Received: May 11, 2023 Revised: August 15, 2023 Accepted: December 11, 2023

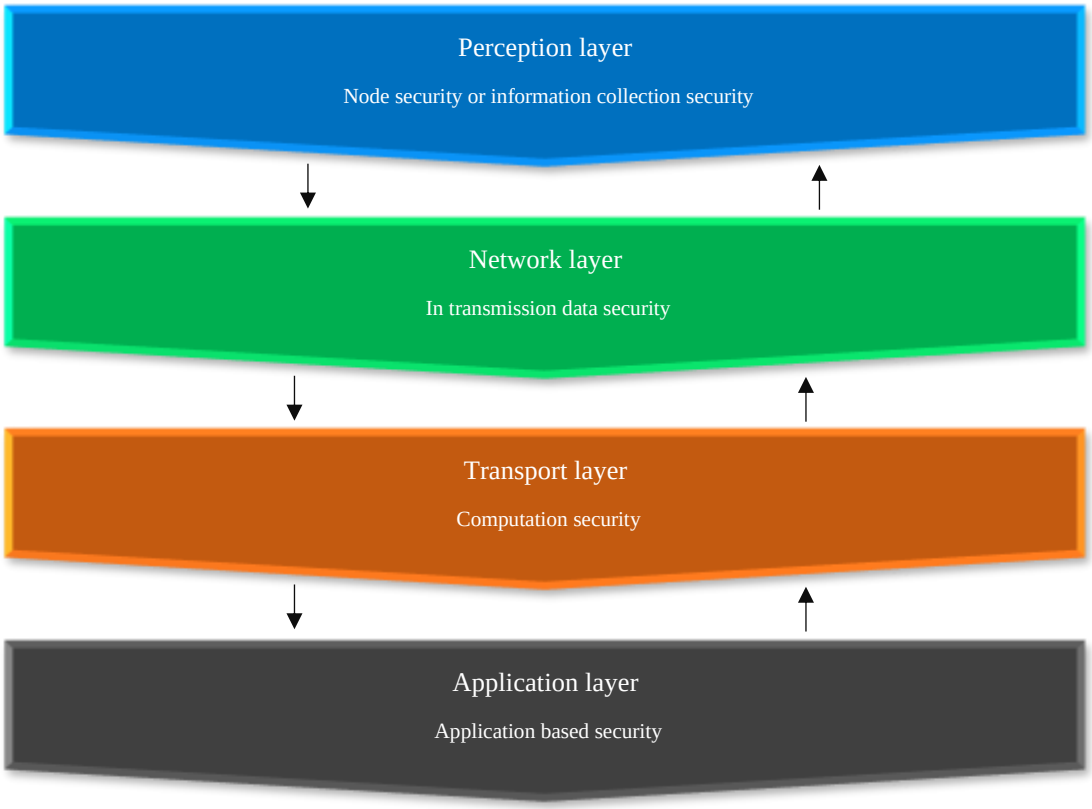

Figure 1: Security Apprehensions at Individual Layer of IoT

In the IoT, devices communicate over the internet to make quick, informed decisions. The capacity, power, and transmission capacity of IoT devices are asset driven [4]. Many scientists are currently trying to pinpoint the problems plaguing the Internet of Things before it can function optimally. Problems plaguing the Internet of Things include:

1) The incompatibility of different kinds of gadgets is the first big problem with the Internet of Things. Different devices have different communication and hardware components. This calls for some sort of middleware to facilitate the exchange of data.
2) As the number of connected devices grows, the Internet of Things will face new threats such as congestion and lag. An IoT network's architecture must be extensible enough to support the addition of new connected devices over time.
3) In the IoT, gadgets are able to exchange data with one another. The network would continue to function normally in the event of the failure of any one component.
4) Different methods are used to store and update data from various origins. When trying to mine information from disparate data sets, you face new difficulties.
5) Concerns about privacy and security in the Internet of Things are exacerbated by the aforementioned problems. A secure communication architecture that protects the privacy of individual devices is essential as the number of heterogeneous devices that need to communicate and share data grows.

Applications of the Internet of Things acquire massive amounts of data because to the interrelation of many things, necessitating cutting-edge security [5]. In terms of protecting the Internet of Things, there are three main axes to consider: applications, systems, and networks. Application security is used to address issues in smart homes, cities, and other similar applications. The same amount of linked items can remain secure and protected thanks to the system's persistent vigilance. Security measures organised in a network contribute to providing safety when communicating over distant connections [6]. As the number of people using the internet grows, it becomes increasingly important for each user to be able to access any data linked with the network. The security aspects of the Internet of Things need special attention because of the vast amounts of data and resources being used.

1) Achieving a secure and reliable communication service for users, devices, and software requires just the fulfilment of a small number of security requirements and criteria.
2) All communications between the source and the recipient should be encrypted. Sensor data is transmitted to the recipient in an encrypted format. However, there is no assurance that the sensor won't reveal the information to an unauthorised party. It is important to secure both the data executives and the development process as a whole.

Doi : https://doi.org/10.54216/JCIM.130104
Received: May 11, 2023 Revised: August 15, 2023 Accepted: December 11, 2023

3) There should be no way for unauthorised objects to change data in transit from one end point to the other. The primary motivation behind mandating integrity checks is to safeguard customer data from unauthorised alteration [7].
4) This is used to establish a connection between things after they have been recognised as being similar. A confirmation system reduces the vulnerability of the system to assault. The validation process faces a formidable obstacle in the form of the need to distinguish between proof procedures for various objects and newly related items.
5) The concept is to provide accessibility as many things are linked to the Internet of Things. Accessibility can extend beyond data to encompass the management of programmes, objects, and resources. IoT items can be monitored with an intrusion identification system to spot any suspicious behaviour.
6) Lightweight, battery-operated security solutions are essential for the deployment of IoT objects with limited resources. Lightweight architectures aren't supposed to be weak; rather, they call for less computing and control capacities throughout development to work flawlessly in the Internet of Things. Because of this, lightweight arrangements perform well in the IoT work for secure utilisation and their length of service.

Given the transient nature of the objects they connect to, data is constantly being transferred between digital and actual items, making them an integral part of the Internet of Things. The Internet of Things incorporates various sensors, RFID tags, and GPS receivers to collect data [8]. Data collection leads to the transformation of raw information into useful data for making educated decisions. The Internet of Things (IoT) is maturing as a scholarly invention used in a wide variety of contexts to make existing systems more efficient and user-friendly. Bandwidth, power, scalability, security, heterogeneity, and privacy are just some of the issues that arise in the Internet of Things. To keep people from losing faith in the Internet of Things, we must first address the privacy and security concerns they may have [9]. Large things communicate with the IoT via the web, and this interaction involves the objects' own data. Therefore, it becomes increasingly important for IoT to ensure the privacy and safety of each user if it is to continue existing as a viable technological advancement.

Because of the current state of IoT security, there are vulnerabilities in every aspect of defence. Therefore, cryptographic solutions are necessary for providing security. The execution time and memory requirements of standard algorithms are too high to work in the IoT. Lightweight algorithms are so essential for the Internet of Things [10].

2. Related Work Done:

It may be deduced that as technology advances, so too does the number of connected gadgets. That's why it's crucial for each gadget to have its own special identifier, thanks to which we can talk to it. The term "internet of things" refers to the network of interconnected gadgets and objects that exchange data in real time [11]. All communication technologies, including the internet, local area networks, wide area networks, radio frequency identification, and sensor systems, should be able to clearly identify, locate, and care for the items [12].

It is mentioned that radio frequency identification (RFID) is employed at the perception layer to uniquely identify things according to the RFID reader's specifications. RFID tags are permanently affixed to every physical object, and when a reader scans one, it instantly updates that object's data. Standardisation is a challenge for IoT because the heterogeneous nature of IoT devices necessitates the use of a standardised reader in order to gather data.

The authors have identified the risks to security posed by RFID technology in the Internet of Things. The blocker tag can cause a denial-of-service assault. This tag's persistent interaction with the reader will hinder its capacity to exchange data with other tags [13-15]. Users' private information and whereabouts are another area of privacy issue. Users' private data may be accessible to third parties without their knowledge or consent.

Some difficulties encountered while employing RFID technology are outlined. One of the primary obstacles is the possibility of signal collision while sending numerous signals from a single reader to multiple tags [16-18]. Tag privacy and security is the second biggest obstacle. Tags are useful for storing data, but they can be compromised by attacks like denial-of-service and eavesdropping if they aren't properly secured.

It is mentioned that sensor systems are another development that can be used in the Internet of Things. Through the use of WSN, information about an event occurring in the real world can be detected and transmitted to a system in order to generate responses [19]. The areas where WSN can be useful include climate control, remote detection, humidity regulation, the military, and disaster management for CEOs. However, WSN only serves to collect data and cannot use such data in any official capacity.

Therefore, IoT takes advantage of WSN's strengths in order to collect data, and then uses that data after it has been prepared to make effective decisions [20-23].

The authors presented a dynamic quality-of-service (QoS) test bench for sensor networks. With this, problems with Contiki OS, such as scalability and cost, will be less severe. As a result, the IoT adopted a WSN-centric approach to data collection, with the intention of using the resulting insights to drive actionable decision-making. The Internet of Things is able to extend the aforementioned use cases for WSN in a more practical way [24].

The current state of the web is effectively transformed by IoT into a thriving, functional web. To this end, IoT manages the widespread availability of various objects equipped with remote technologies such as Bluetooth,

Doi : https://doi.org/10.54216/JCIM.130104
Received: May 11, 2023 Revised: August 15, 2023 Accepted: December 11, 2023

RFID, or sensors. A user must implement a remote innovation dependent on the IoT's practical domain [25]. Bluetooth can be chosen in situations where the Internet of Things's operational zone is indoors only, as in the automated management of phone calls. RFIDs are chosen for uses where it is necessary to maintain data for each object on a unique RFID tag. Thus, in applications such as stock management, an RFID reader is used to retrieve information from the tag [26]. Finally, sensors-based technology is used in most IoT applications today, including smart homes, smart cities, traffic management systems, and more. Some examples of sensors that could be employed are motion, proximity, temperature, and others. At present, Alexa from Amazon is being actively promoted, which employs the method of voice directions for web-connected IoT products.

3. Motivation for the Research Work:

In a recent literature review, many researchers recommended lightweight symmetric and asymmetric security solutions for the Internet of Things (IoT). Symmetric arrangements provide privacy and authenticity with small key sizes and a lack of complexity, but they do not provide authentication, and the distribution of keys is a difficult operation. But while deviating computations provide privacy, integrity, and validity, their complexity and unsuitability for mandatory IoT use cases make their key sizes too large. Therefore, there is a need for secure computation, which makes a point of emphasising lightweight symmetric and asymmetric solutions to a greater extent; these solutions may require less investment for execution in addition to ideal energy requirements, and they will ultimately guarantee full security administrations like secrecy, trustworthiness, and realness.

4. The Proposed Work:

The recommended security architecture offers services for data secrecy and authentication. It does this by using a cutting-edge method of authentication in conjunction with a cryptographic algorithm to ensure security. This paper evaluates the proposed HLSF against the current frameworks by completing the authentication, secure data collecting, and decision making process. The parameters used to assess performance include throughput, packet delivery ratio, and latency.

The security architecture of an organisation must abide by its own rules and specifications. When assessing a security framework, factors like secrecy and authentication are looked at. Next in the evaluation of a framework is confirming the accuracy of the collected data. The last criterion for assessing a security system is data synthesis or mining for insightful judgements. Within a security framework, competence is the capacity to meet security requirements and make timely, effective judgements.

The general equation for Linear Regression (LR) model is:

$$Y = \beta 0 + \beta 1X1 + \beta 2X2 + \cdots + \beta nXn + \epsilon \quad (1)$$

where Y is the predicted variable, $X1\ to\ Xn$ are predictor variables, 0 is the intercept, 1 to n are coefficients, and ϵ is the error term.

$$Map\ (key1, value1)\ \rightarrow\ list\ (key2, value2) \quad (2)$$

$$Reduce\ (key2, list\ (value2))\ \rightarrow\ list\ (output\_key, output\_value) \quad (3)$$

$$Execution\ Time\ =\ End\ Time\ -\ Start\ Time \quad (4)$$

The proposed approach is based on these mathematical formulas and algorithms, which allow computational scientists to take use of data-driven approaches.

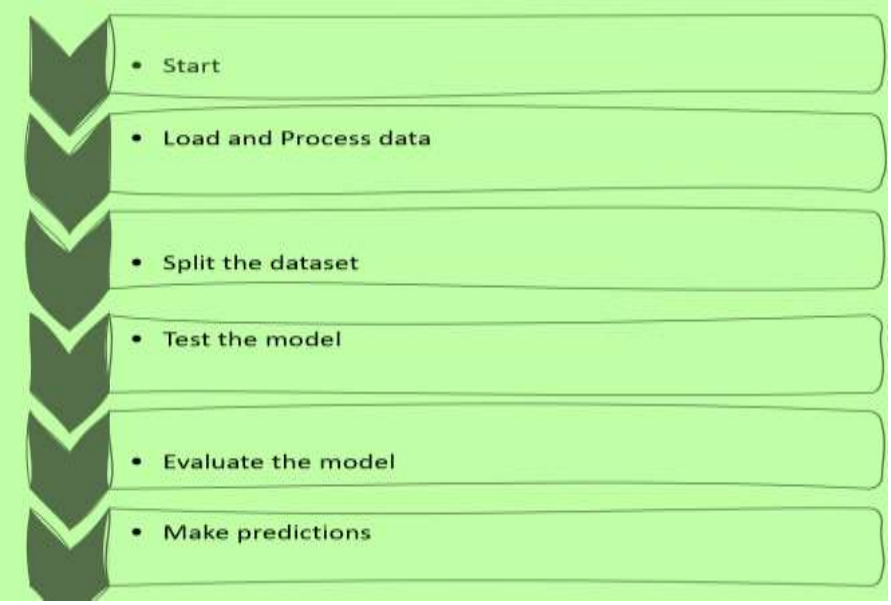

Figure 2: Machine Learning Algorithm Flowchart.

Doi : https://doi.org/10.54216/JCIM.130104
Received: May 11, 2023 Revised: August 15, 2023 Accepted: December 11, 2023

People's lifestyles have drastically changed as a result of the Internet of Things. Every IoT-enabled device operates intelligently, increasing our reliance on technology in all facets of our lives. The domains of inventory management, healthcare, and smart home technologies are just a few of the numerous real-world applications for the Internet of Things. Because they anticipate the Internet of Things to offer a high degree of privacy and safety, users are looking for a security framework. The IoT's built-in security solutions are vulnerable to several threats, such as spoofing and denial-of-service attacks. The security architecture of an organisation must abide by its own rules and specifications. When assessing a security framework, factors like secrecy and authentication are looked at. Next in the evaluation of a framework is confirming the accuracy of the collected data. The last criterion for assessing a security system is data synthesis or mining for insightful judgements. Within a security framework, competence is the capacity to meet security requirements and make timely, effective judgements. A security architecture often guarantees the overall security of a system.

It is possible for one device to take on the role of client while another device takes on the role of server in a CoAP-based restricted network, such as the Internet of Things. You might think of CoAP as an internet version of the Hyper Text Transfer Protocol (HTTP). CoAP use URLs to reference resources. A CoAP server, when implemented correctly, can also serve as a proxy gateway, allowing an HTTP client to access the CoAP server's resources. CoAP's incorporation into the web is depicted in Figure 3. Since CoAP itself constitutes the private network, only the CoAP server is capable of handling requests from CoAP clients. Since CoAP is a subset of HTTP, it can be expanded to handle requests from HTTP clients by means of a CoAP/HTTP mapping mechanism. As can be seen in Figure 3, this link can be set up with the help of a 6LoWPAN border router (6LBR).

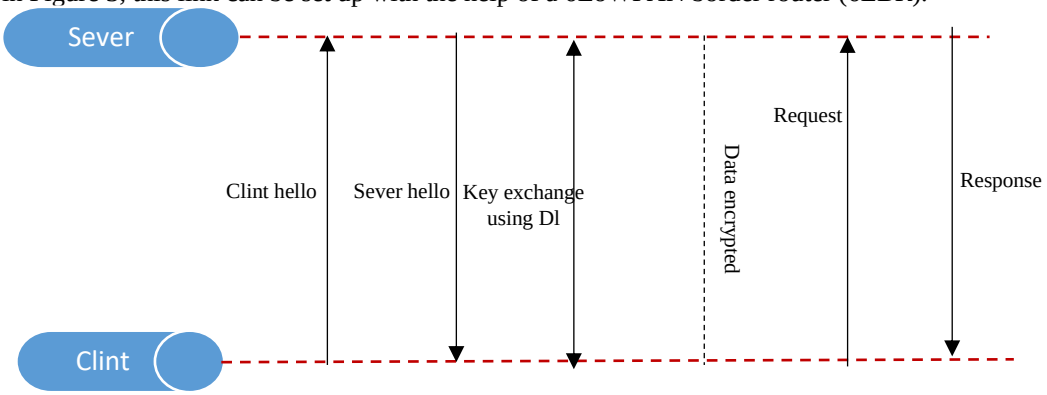

Figure 3: Pre shared Key option of CoAP

There are three stages to the proposed HLSF: registration, authentication, and the LDS. Key sharing is used to distribute authentication credentials to newly joined devices after they have been registered with the server. Once the device has the credentials, mutual authentication is performed between the device and the server before any communication is initiated. After a device has been verified, the data sent to and from it is encrypted using the LDS algorithm.

4.1. Registration Phase:

The following are the stages of registration:

1. Device Di will present its IDD to the IS through a safe channel, starting the process of establishing a connection between the two devices.
2. IS calculates a nonce value NS after receiving the connection request from Di. A shared key KS is then calculated as follows: KS= IDD ⊕ h(IDD|| NS).
3. Alongside this, IS generates a collection of alternate keys Ka= ka_1, ka_2,....ka_n relative to each uidi UID and a set of unique-Ids, UID= id1, id2, id3,....idn.
4. It involves a random sequence number (SN) being generated by IS. IS creates KS, unique Ids, alternate keys, and SN for each request sent by the Di. In the event that Di re-issues a request to IS, a fresh SN will be created. IS is responsible for sending the same SN that is stored in the database to the Di. Using SN helps prevent the intruder from injecting a repeat of the conversation.
5. As a final preparatory step before beginning the authentication process, IS compares the SN sent by Di with the one in the database. If a match is found, the second phase of authentication will take effect. If no match is found in SN, IS disconnects Di and suggests that it instead use one of the UID and Ka pairs. After this pair has been used, the information about them will be deleted from both IS and Di. At the conclusion, IS sends an encrypted message to Di using Di's public key, which contains a set of values (KS, idi, kai, and sn), and IS stores these values (together with Di's ID, IDD), in its own database.

4.2. The Authentication Process

Di and IS undertake mutual authentication with each other throughout the authentication step. The following are the stages of the authentication process:

Doi : https://doi.org/10.54216/JCIM.130104
Received: May 11, 2023 Revised: August 15, 2023 Accepted: December 11, 2023

1. Di uses the nonce value N1 to produce a variable using the formula V1 = h(IDD || KS ⊕ N1).
2. Di composes a request message to the IS with the format "V1, IDD, SN."
3. Third, if SN is unavailable, Di will use one of the pairs (idi, kai) in which kai can stand in for KS.
4. when IS receives a request from Di, it checks to see if the SN included inside it corresponds to the SN of the associated Di stored in the database, and it also checks to see if the other parameters are legitimate. IS then determines N1's value.
5. Assuming all parameters check out, IS will take a nonce value N2, construct a new random sequence number SNnew = h (IDD || KS || N1) ⊕ SN, and calculate a temporary variable TV = h (IDD || KS || N2) ⊕ SNnew, as well as a computing variable V2= h(IDD || KS || N1|| TV) if all goes well.
6. This step is for Di to compare V2 with the computed value h(IDD || KS || N1|| TV) upon receiving the message "V2, SNNew, TV" from the IS. Di finds the nonce N2 if a match occurs by utilising the formula TV = h (IDD || KS || N2) ⊕ SNnew.

4.3. LDS Algorithm for Lightweight Data Security

After Di and IS have successfully completed mutual authentication, data security via encryption mechanism can be provided. Each data block is 64 bits in size, and the combined KS size of Di and IS is 128 bits. Lightweight Data Security (LDS) is a suggested algorithm for providing this safety feature. This algorithm handles encrypted data transmission and provides security services like data encryption and data integrity verification.
Mathematical equation of LDS Algorithm are as follows:

1. Generator Loss: $LG=-\mathrm{E}z[\log D(G(z))]$ (5)
2. Discriminator Loss:
   $LD=-\mathrm{E}x[\log D(x)]-\mathrm{E}z[\log(1-D(G(z)))]$ (6)
3. LSTM Forecasting Equation:
   $St+1=LSTM(St,St-1,...,St-n)$ (7)
4. Markov Chain Transition Probability:
   $P(St+1=s'|St=s)$ (8)
5. GAN Generator Output: $G(z)$
6. Discriminator Output: $D(x)$
7. Random Noise Input: z
8. Sequence of Past Threat Scenarios',$St-1,...,St-n$

The goal of this suggested technique is to enhance the accuracy and efficacy of

The proposed LDS uses the Add, Rotate, and XOR (ARX) operations to complete its work in 20 cycles. The user can decide how many times the process should run in order to achieve full diffusion, with consideration given to the necessary execution time. Taking into account the IoT application environment, the three ARX procedures were selected because they provide the best security trade-off together with a lightweight solution. Twenty rounds of ARX operations and a key generation function are shown to represent the structure of LDS.

5. Result and Discussion:

There are a wide variety of data types that can be managed by data mining techniques when applied to application settings. The literature contains a number of research that deal to association rules, clustering, and classification-based mining approaches. These investigations may be found in the literature. Based on the outcomes of the study, it seems that more algorithms that are developed based on the methodologies that were discussed before might potentially be useful in the Internet of Things. Clustering is accomplished via the utilisation of the k-means clustering approach, classification is accomplished through the utilisation of the k-nearest neighbour (kNN) methodology, and association rule-based mining is accomplished through the utilisation of the FP (frequent pattern) growth method. All of these approaches are now being used. For the aim of determining which of the four decision makers for the Internet of Things is the most effective and productive, the objective of this study is to evaluate three different mining methodologies. Our evaluation of the kNN, k-means, and FP algorithms is based on the recall value, accuracy, and precision of their respective outcomes. This allows us to compare and contrast these techniques. For the purpose of evaluation, the performer who obtained the highest score will be selected via the use of both the HLSF and the CoAP.

5.1. Precision

The proportion of valid observations relative to the total number of observations is the definition of an accurate measurement. Accuracy ratio is the term that is used to describe this relationship. One of the factors that is related with an improvement in the accuracy of a DM technique is an increase in the number of events that are correctly recognised. As a consequence of the accuracy evaluations that were carried out on the kNN, k-means, and FP algorithms, the following are the findings of those evaluations. Figure 4 and Table 1 both provide these results in their respective formats. Figure 3 shows that when the number of iterations is varied, the FP method achieves a higher percentage of accuracy than kNN and k-means cluster algorithms.

Table 1: Precision Based Analysis of KNN, K-Means and FP In IoT.

S. No.	Iteration Count	kNN	k-means	FP

Doi : https://doi.org/10.54216/JCIM.130104
Received: May 11, 2023 Revised: August 15, 2023 Accepted: December 11, 2023

1	2	95.367	96.485	95.931
2	4	93.716	96.247	96.548
3	6	93.082	95.505	94.871
4	8	96.243	96.923	97.148
5	10	91.758	92.673	94.872

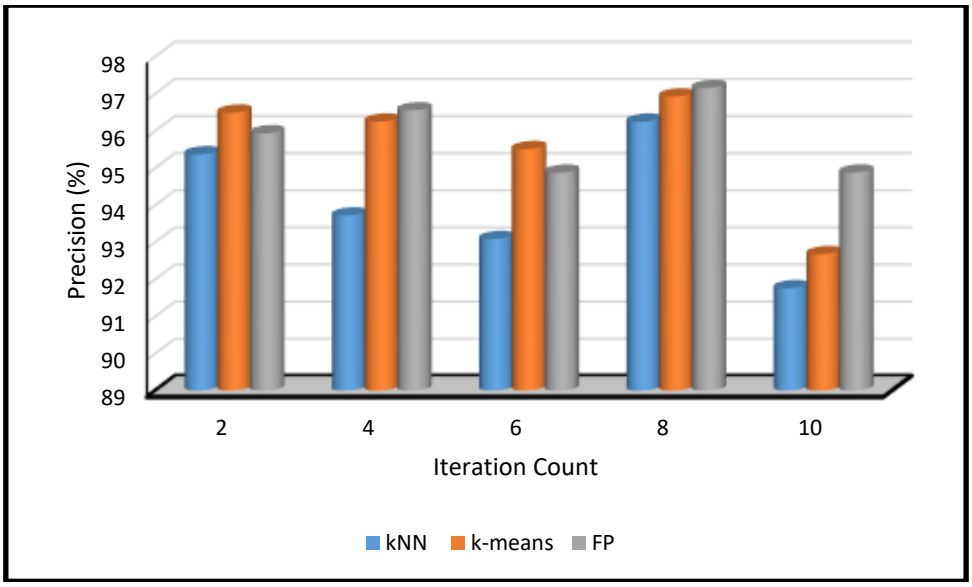

Figure 4: Precision Based Analysis of Knn, K-Means and FP In IoT.

5.2. Accuracy:

The amount of correctly recorded occurrences free of systematic errors (Type 1 and Type 2) is the accuracy. A DM technique's accuracy is directly proportional to the number of correctly gathered instances. Table 2 and Figure 5 below illustrate the results of the accuracy evaluations of the kNN, k-means, and FP algorithms, respectively. When compared to kNN and k-means cluster algorithms, the FP algorithm achieves a higher percentage of accuracy with a variable number of repetitions.

Table 2: Accuracy Based Analysis of KNN, K-Means and FP In IoT.

S. No.	Iteration Count	kNN	k-means	FP
1	2	96	98	98
2	4	94	96	97
3	6	96	97	98
4	8	98	97	98
5	10	92	94	95

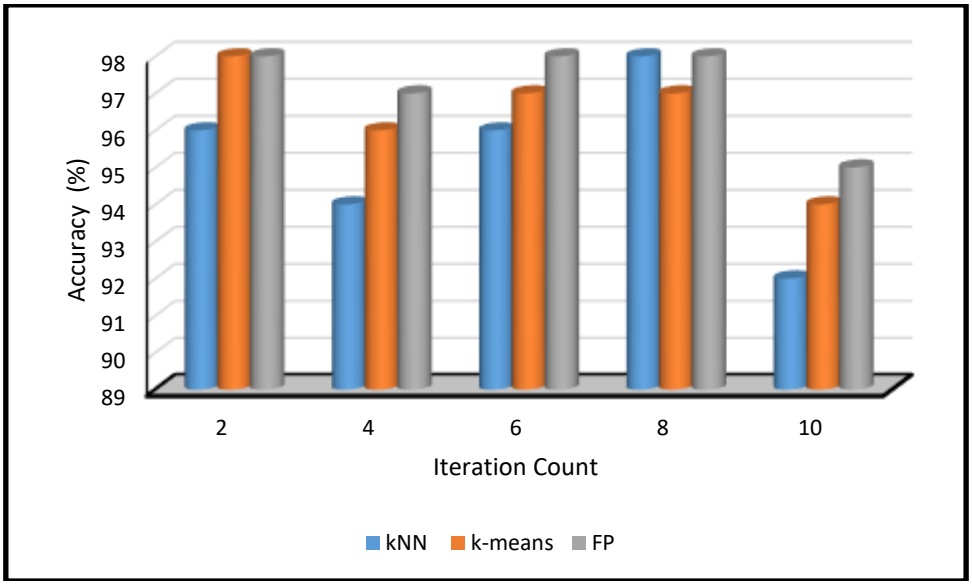

Figure 5: Accuracy Based Analysis of kNN, K-Means and FP in IoT.

Doi : https://doi.org/10.54216/JCIM.130104
Received: May 11, 2023 Revised: August 15, 2023 Accepted: December 11, 2023

5.3. Recall:

When comparing the number of true occurrences gathered with the number of true occurrences that would have been collected, the ratio is called recall. An improved DM technique's recall is achieved by collecting the highest amount of relevant instances. Recall performance of the kNN, k-means, and FP algorithms is compared in Table 3 and illustrated in Figure 6 below. When compared to kNN and k-means cluster algorithms, the recall percentage of the FP algorithm is higher throughout a range of iterations. As compared to other algorithms, the FP method has higher precision, accuracy, and recall, according to the performance metrics that were analysed.

Table 3: Recall Based Analysis of kNN, K-Means and FP In IoT.

S. No.	Iteration Count	kNN	k-means	FP
1	2	94.57	95.38	96.82
2	4	96.15	97.59	98.29
3	6	96.38	97.53	98.19
4	8	95.47	95.86	97.28
5	10	96.28	97.43	97.94

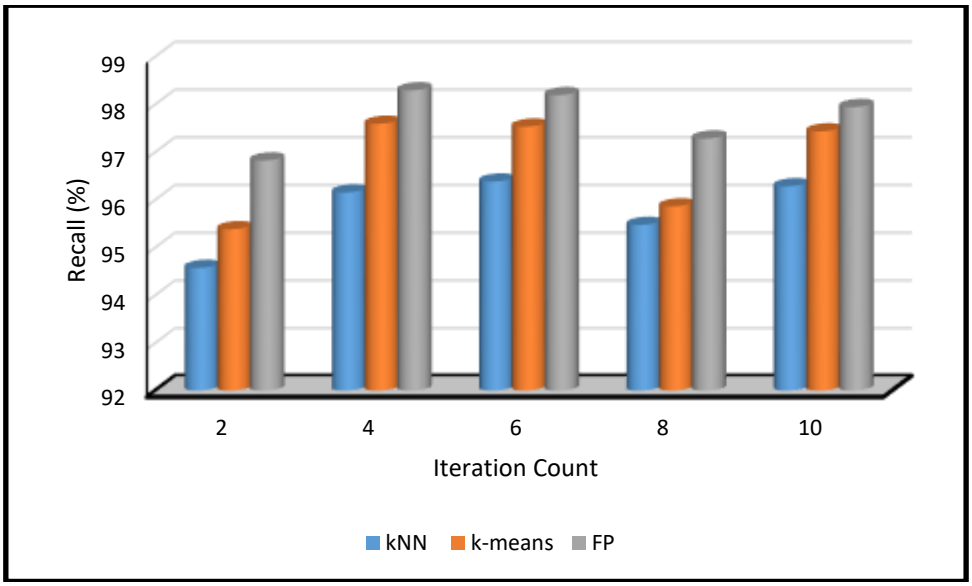

Figure 6: Recall Based Analysis of kNN, K-Means and FP in IoT.

There are two ways in which the Internet of Things scenario is applied in this study. One, when HLSF security mechanisms are used for data collection. Secondly, when COAP is used as a security measure during data collection. In order to determine the recall, accuracy, and precision, data mining is then used in both cases. Two scenarios with HLSF and CoAP security are shown in Figure 7, together with the percentages of recall, accuracy, and precision.

Table 4: Evaluation parameters comparison of the proposed method with existing approach.

Iteration Count	Precision		Accuracy		Recall	
	COAP	HLSF	COAP	HLSF	COAP	HLSF
2	96.43	99.14	98.28	98.39	96.38	99.19
4	97.86	98.59	97.28	99.16	98.29	99.37
6	95.48	98.16	98.28	98.37	98.47	98.52
8	97.28	97.31	98.38	98.47	96.49	97.38
10	95.82	97.38	95.28	97.39	95.68	96.91

Doi : https://doi.org/10.54216/JCIM.130104
Received: May 11, 2023 Revised: August 15, 2023 Accepted: December 11, 2023

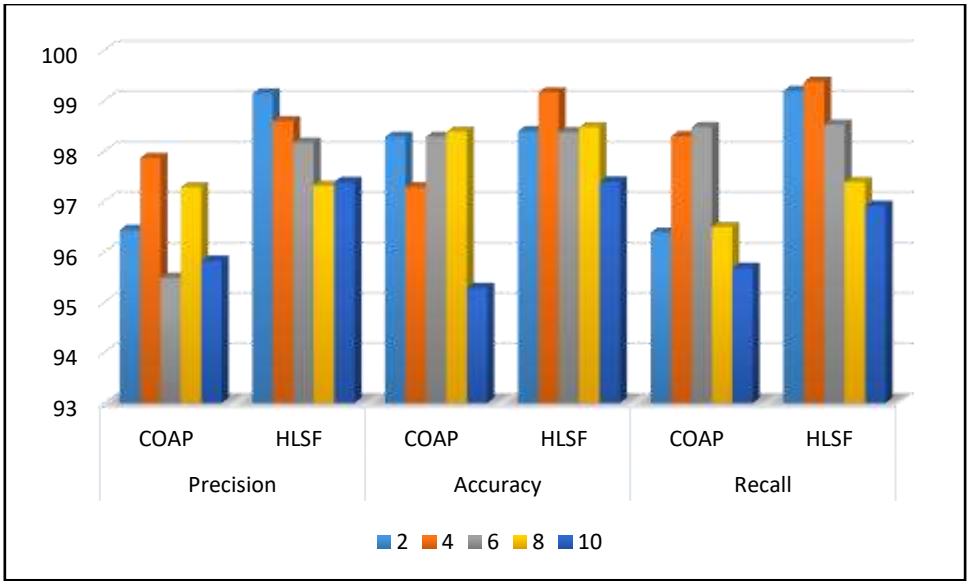

Figure 7: Evaluation parameters comparison of the proposed method with existing approach.

According to the findings, the HLSF framework that was proposed effectively utilises precision, accuracy, and recall in the process of data production, which ultimately results in improved decision-making.

6. Conclusion:

It is necessary for the security framework of any firm to adhere to the laws and regulations that are specific to that company. Within the scope of this discussion, we are assessing a security framework based on the authentication and confidentiality capabilities it has. As part of the evaluation process for a framework, the following step is to check the accuracy of the data that was obtained. In conclusion, one of the assessment metrics for a security system is the capability to mine or synthesise data in order to make judgements that are beneficial. It is possible to consider a security framework to be competent if it is able to make decisions in real time and be successful in doing so while still meeting all security criteria. This article shows the results and examines the techniques of data mining in relation to the Internet of Things (IoT) and the HLSF architecture. Specifically, the presentation focuses on the findings. We begin by analysing three well-known data mining techniques that make use of the PAIR (Precision, Accuracy, and Recall) measure. These techniques are k-nearest neighbours, k-means, and FP. Among all of the mining strategies that were put to the test, the FP technique produced the most favourable outcomes. After that, FP is used in two distinct Internet of Things (IoT) situations: one with the HLSF framework, and another with CoAP as security measures. Both of these scenarios are described below. These findings demonstrate that the HLSF framework that was proposed makes more effective use of precision, accuracy, and recall when it comes to the production of data, which ultimately results in improved decision-making.

References

[1]. JS. Silva, P. Zhang, T. Pering, F. Boavida,T. Hara,NC. Liebau, ―People-centric internet of things, IEEE Communications Magazine, vol. 55, no. 2, pp-18-19, Feb. 2017.
[2] A. Whitmore, A. Agarwal,L. Da Xu, ―The Internet of Things—A survey of topics and trends, Information Systems Frontiers, vol. 17, no. 2, pp. 261-274, Apr. 2015.
[3] AK. Luhach AK, SK. Dwivedi, CK. Jha, ―Applying SOA to an E-commerce system and designing a logical security framework for small and medium sized E-commerce based on SOA, In 2014 IEEE International Conference on Computational Intelligence and Computing Research, pp. 1-6, Dec. 2014.
[4]. M. Chernyshev, Z. Baig, O. Bello, S. Zeadally, ―Internet of Things (IoT): research, simulators, and testbeds,‖ IEEE Internet of Things Journal, vol. 5, no. 3, pp. 1637-1647, Jun. 2018.
[5] R. Hamidouche, Z. Aliouat, AM. Gueroui, AA. Ari, and L. Louail. "Classical and bio-inspired mobility in sensor networks for IoT applications." Journal of Network and Computer Applications, Jul. 2018.
[6]. S. Ezdiani, I.S. Acharyya, S. Sivakumar, A. Al-Anbuky, ―An IoT environment for WSN adaptive QoS,‖ In 2015 IEEE International Conference on Data Science and Data Intensive Systems, IEEE, pp. 586-593, Dec. 2015.
[7] J. Liu, Y. Li, M. Chen, W. Dong, D. Jin, ―Software-defined internet of things for smart urban sensing,‖ IEEE communications magazine, vol. 53, no. 9, pp. 55-63, Sep 2015.

Doi : https://doi.org/10.54216/JCIM.130104
Received: May 11, 2023 Revised: August 15, 2023 Accepted: December 11, 2023

[8]. F. H. Bijarbooneh, W. Du, E.C Ngai, X. Fu, J. Liu, ―Cloud-assisted data fusion and sensor selection for internet of things, IEEE Internet of Things Journal, vol. 3, no. 3, pp. 257-268, Jun 2016.
[9] A. Rajeswari, R. Manavalan, ―Data collection methods in wireless sensor network: A study, Int. J. Res. Appl. Sci. Eng. Technol, pp. 259-282, Sep. 2014.
[10]. Y. Yang, H. Peng, L Li, and X. Niu. "General theory of security and a study case in internet of things." IEEE Internet of Things Journal, vol. 4, no. 2, pp. 592-600, Apr. 2017.
[11]. H. Hellaoui, M. Koudil, A. Bouabdallah, ―Energy-efficient mechanisms in security of the internet of things: A survey,‖ Computer Networks, pp. 173-189, Nov. 2017.
[12] D. He, R. Ye, S. Chan, M. Guizani, and Y. Xu. "Privacy in the Internet of Things for Smart Healthcare," IEEE Communications Magazine, vol. 56, no. 4, pp. 38-44, Apr. 2018.
[13] W. Li, H. Song, and F. Zeng. "Policy-based secure and trustworthy sensing for internet of things in smart cities," IEEE Internet of Things Journal, vol. 5, no. 2, pp. 716-723, Apr. 2018.
[14] Y. Kawamoto, H. Nishiyama, N. Kato, Y. Shimizu, A. Takahara, and T. Jiang. "Effectively collecting data for the location-based authentication in Internet of Things," IEEE Systems Journal, vol. 11, no. 3, pp. 1403-1411, Sep. 2017.
[15]. Anuradha, M.; Jayasankar, T.; Prakash, N.; Sikkandar, M.Y.; Hemalakshmi, G.; Bharatiraja, C.; Britto, A.S.F. IoT enabled cancer prediction system to enhance the authentication and security using cloud computing. Microprocess. Microsyst. 2021, 80, 103301.
[16]. Irshad, A.; Usman, M.; Chaudhry, S.A.; Bashir, A.K.; Jolfaei, A.; Srivastava, G. Fuzzy-in-the-Loop-Driven Low-Cost and Secure Biometric User Access to Server. IEEE Trans. Reliab. 2020, 70, 1014–1025. [17]. Chaudhry, S.A.; Farash, M.S.; Kumar, N.; Alsharif, M.H. PFLUA-DIoT: A pairing free lightweight and unlinkable user access control scheme for distributed IoT environments. IEEE Syst. J. 2020, 16, 309–316.
[18]. Mishra, N.; Pandya, S. Internet of Things Applications, Security Challenges, Attacks, Intrusion Detection, and Future Visions: A Systematic Review. IEEE Access 2021, 9, 59353–59377.
[19]. Hameed, A.; Alomary, A. Security issues in IoT: A survey. In Proceedings of the 2019 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT), Sakhier, Bahrain, 22–23 September 2019; pp. 1–5.
[20]. Lu, Y.; Da Xu, L. Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics. IEEE Internet Things J. 2019, 6, 2103–2115.
[21]. Hassija, V.; Chamola, V.; Saxena, V.; Jain, D.; Goyal, P.; Sikdar, B. A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures. IEEE Access 2019, 7, 82721–82743.
[22]. Jurcut, A.; Niculcea, T.; Ranaweera, P.; Le-Khac, N.-A. Security Considerations for Internet of Things: A Survey. SN Comput. Sci. 2020, 1, 1–19.
[23]. Kouicem, D.E.; Bouabdallah, A.; Lakhlef, H. Internet of things security: A top-down survey. Comput. Netw. 2018, 141, 199–221.
[24]. Sha, K.; Yang, T.A.; Wei, W.; Davari, S. A survey of edge computing-based designs for IoT security. Digit. Commun. Netw. 2020, 6, 195–202.
[25]. Yousefnezhad, N.; Malhi, A.; Främling, K. Security in product lifecycle of IoT devices: A survey. J. Netw. Comput. Appl. 2020, 171, 102779.
[26]. Yugha, R.; Chithra, S. A survey on technologies and security protocols: Reference for future generation IoT. J. Netw. Comput. Appl. 2020, 169, 102763.

Doi : https://doi.org/10.54216/JCIM.130104
Received: May 11, 2023 Revised: August 15, 2023 Accepted: December 11, 2023