Journal of Information Systems Engineering and Management
2025, 10(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

A Novel Hybrid FSO-SVM Model for Attack Detection and Classification in Social IoT

Maniveena.C[1], Kalaiselvi.R[2]

[1]Research Scholar, Department of Computer Science &Engineering, Noorul Islam Centre for Higher Education (Deemed to be University) Thuckalay, Kanyakumari (District), Tamil Nadu, India.

maniveenac@gmail.com

[2] Professor and Head, Department of Computer Applications, PET Engineering College, Vallioor, Thirunelveli (District), Anna University, Chennai, India.

kalaiselvir32@gmail.com

ARTICLE INFO

Received: 15 Nov 2024

Revised: 28 Dec 2024

Accepted: 15 Jan 2025

ABSTRACT

Modern Society has multiple channels of communication therefore, multiple ways are there to promote sociability and social relationships which offer the construction of social identities. Among all of these methods, the internet seems to be a potent instrument for modern society's communication. The term "Social Internet of Things" infers to a novel strategy that applies the Social Network Paradigm to the Internet of Things (IoT) domain, facilitating communication while enhancing the relationship between users and devices. A secure communication can be provided by using a novel hybrid classification approach which is developed by combining the benefits of SVM and FSO. FSO is an innovative approach that combines AI strategies with clarified and enhanced security processes. SVM stands out as an essential and popular classification method. SVM performance is highly dependent on choosing the most important characteristics and determining kernel settings effectively. The FSO procedure is also notable for updating positions through element-wise Hadamard matrix multiplication processes. By allowing for simultaneous processing on several data items, this operation shortens the computation time overall. Microsoft Research Paraphrase Corpus datasets are used to evaluate the proposed model, and compared with several well-known metaheuristic algorithms that have used to enhance the performance of SVM. Many attack datasets are used in widespread experiments to verify this system. The results are compared based on performance metrics such as accuracy, precision, recall and F1-score. The proposed framework gains a 99.2% overall classification accuracy.

Keywords: Social IoT, FSO Algorithm, AI, ML, SVM, Quantum Key Distribution.

1. INTRODUCTION:

Through a steady stream of new IoT gadgets reaching the market, IoT stands out as one of the industries in today's digital environment that is growing at the fastest rate. These electronic devices are clever and internet-connected. Convolutional Neural Networks (CNN), however, usually can't keep up with the needs of this dynamic environment because the IoT is constantly evolving and dynamic. It becomes essential to set up a highly secure and dynamic network architecture in order to enable IoT operations. Among the many applications of IoT are smart cities and smart homes; other applications include industry automation and education [1]. The vast scope of IoT networks raises a number of new concerns, including managing enormous volumes of data, managing device management, guaranteeing sufficient storage and computational capacity, promoting smooth communication, and maintaining strict security and privacy standards.

Most IoT smart devices are handled by humans for most of the day. In order to attract attention, smartphone users frequently share first-hand information on social media sites like Facebook. As a result, it becomes imperative to look into how social traits like curiosity, dependability, and interaction history might be incorporated into the IoT. This idea gives rise to the concept of the Social Internet of Things (Social IoT), which imagines a cooperative setting in which intelligent objects can interact with one another and share information with their surroundings [2]. As the modern threat landscape evolves, Artificial Intelligence (AI) into a security strategy is becoming increasingly important for building and maintaining a secure posture. Making computer think like humans is the goal of AI. The digital transformation of industries will accelerate due to this breakthrough [3].

Data security is a significant concern, and there is a risk of data explosion due to the rapid development of the Social IoT ecosystem. To comprehend and manage developments in the Internet of Things, security models must be updated on a regular basis. Consequently, most approaches to Social IoT fail. Methods related to AI and Machine Learning (ML) are thus proposed as solutions to the Social IoT security issue. Analysing typical or problematic Social IoT interactions can be done with ML and Deep Learning (DL) approaches. By using simple derivations and mutations of prior attacks, these systems are able to forecast new attacks [4].

2. LITERATURE REVIEW:

Punithavathi, P., et al. (2019), presented a framework for a cloud-based, lightweight cancellable biometric authentication solution. The results of the study indicated that the proposed approach might find use in real-world scenarios (i.e., be able to authenticate client devices with low overhead and high precision without jeopardizing the privacy of the private biometric templates in the cloud environment). When compared to state-of-the-art techniques, theoretical and empirical study shows that the proposed approach has a low equivalent error rate. Furthermore, it has been shown that the proposed approach takes less time, making it appropriate for usage in Internet of Things applications [5].

Newaz, A. I., et al. (2019) introduced Health-Guard, a unique machine learning-based security framework for identifying harmful actions in a Smart Healthcare System (SHS). Vital signs are monitored by all connected devices in a SHS, and the data is correlated to comprehend changes in biological function and distinguish between benign and malignant actions. Health-Guard uses four machine learning-based detection methods (k-Nearest Neighbour, Decision Tree, Random Forest, and Artificial Neural Network) to find risky activities in a SHS. Using information from eight distinct smart medical devices, they trained Health-Guard for twelve benign events, including seven ordinary user behaviours and five events related to sickness. The efficacy of Health Guard against three more serious hazards was also assessed by the study. Health-Guard is an effective security architecture for SHS, according to our comprehensive evaluation, which yielded a 91 percent accuracy rate and a 90 percent F1 score [6].

In order to develop a secure content sharing (SCS) system that balances security and quality of experience (QoE), Wang, B., et al. (2020) investigated social trust. First, based on the suggested "User-Content-Social Group" graph that depicts users' preferences over time, social trust is dynamically forecasted using the random walk approach. The paper proposed a hierarchical game model based on the social trust value to split the optimization problem into two smaller problems: user pairing and channel selection. Since the user pairing sub-problem is stated as a matching sub-game with peer effect, the embedded rotation-swap matching algorithm can accommodate the mutual interference dynamics. The directed hypergraph, which is shown to be an exact potential game, serves as the game space for the second subproblem, which may be expressed as a safe channel selection sub-game. Next, researchers find the optimal sub-global game by searching for the best pure Nash equilibrium using an uncoupled-user concurrent learning algorithm (UUCL). Ultimately, simulation results using a real-world social dataset indicated that our proposed approach might greatly increase security while maintaining user quality of experience (QoE) [7].

The proliferation of mobile devices poses a threat to the security and privacy of the 5G IoT frameworks. In this paper, Ullah, F., et al. (2021) proposed a hybrid solution to the Control Flow Graph (CFG) and a

deep learning model to secure the smart services of the 5G-IoT framework. Once the newest provided APK file has been extracted, Java source files from possibly original and duplicated programs can be obtained using the JDEX decompiler. Secondly, the source files consist of multiple Android-based components. During the creation of the CFGs, the weighted characteristics of each component are extracted. In the end, features from various Android application sections are used to train the Recurrent Neural Network (RNN), which then predicts possibly cloned applications. According to experimental results, the suggested method may be able to clone apps from multiple Android app marketplaces with an average accuracy of 96.24 percent [8].

Karthik, E., &Sethukarasi, T. (2022), introduced a novel long short-term memory (FSO-LSTM) architecture based on firebug swarm optimization for identifying sardonic sentiments in tweets. The suggested FSO-based LSTM architecture is trained on the CK + dataset in order to recognize the users' facial emotions. The Fire bug Swam Optimization technique is used to optimize the weighting parameters of the LSTM architecture, hence reducing the mean absolute error and root-mean-square error. Comparing the proposed method to the most advanced methods, the categorization accuracy is on average 97.25 percent [9].

3. PROBLEM STATEMENT:

The upcoming communication revolution is symbolized by IoT. Security is a crucial component of the present IoT implementation because anyone can intentionally or unintentionally target other users' content sharing on the same channel. IoT can be used to provide physical objects the ability to easily generate, receive, and share data. Many IoT apps are designed to automate various processes with the goal of enabling inanimate devices to function independently, without the need for human interaction. These existing and emerging IoT operations hold immense promise in enhancing user comfort, efficiency and automation levels. However, realizing a world where such advancements proliferate necessitates robust measures in security, privacy, authentication and resilience against potential attacks. Once a security attack has been identified, an effective defence mechanism must be considered to prevent the attacker from causing harm.

Support Vector Machine (SVM)

Among the leading widely used classification methods in ML is SVM. This have many uses in fields like text categorizing and image classification. Both feature selection and kernel variable setting are crucial steps in the SVM training phase that have a big impact on the classification performance of the model [10].

Assume that a training dataset $(u_i, v_i)\}_{j=1}{}^{m} \in L^n \times (-1,1)$ is provided, with $u_i \in L^n$ serving as the input vector and v_i 1 or – 1 serving as the emphasize regard or identification. Then, by optimizing the subsequent equation (Eq.1), the issue of determining the ideal hyperplane could be resolved.

$$min_{r,c,\varepsilon} \frac{1}{2} w^T w + D(\sum_{j=1}^{m} \rho_j \varepsilon_j) \qquad (1)$$

$$v_i[w^T . \varphi(v_i) + c] \geq 1 - C\varepsilon_j$$

$$\rho_j > 0, \varepsilon_j > 0, j = 1,2, \ldots . m$$

The regression coefficient vector, the impact parameter, the estimation error assesses in the SVM, and the erroneous measure with various proportions are represented by the variables w, D, ε_j, and $\rho_j \varepsilon_j$, in the equation, respectively. A conversion also done by the function [11]. Large range multipliers were employed in the following stage to convert the issue into an additional one (Eq. 2).

$$max_{\vartheta} = \frac{1}{2} \sum_{k=1}^{m} \sum_{l=1}^{m} \beta_k \beta_l v_k v_l J(u_k v_l) \quad (2)$$

$$\beta_k{}^{*}(v_i(w^{*} . \varphi(u) + c*) - 1 + \varepsilon_j{}^{*}) = 0,$$

$$(\rho_j D - \varepsilon_j{}^{*} = 0; k = 1,2, \ldots \ldots, m) \qquad (3)$$

The optimum result in the above equation is (.)*, and a support vector is defined as the uk point with the corresponding k > 0. In order to generate a more suitable execution, the kernel function $J(u_k v_l)$is also regarded as a Gaussian function (Eq. 4).

$$J(u_k v_l) = \exp\left(-\beta \left\| u_k - v_l \right\|^2\right) \quad (4)$$

Two parameters D must be pre-adjusted in the SVM with the kernel's Gaussian function in order to have accurate forecast accuracy. The trade-offs between minimizing the estimation error and minimizing the model complexity are demonstrated by the first variable, D. The Gaussian kernel's width is determined by the second variable β.

Firebug Swarm Optimization (FSO)

FSO and computational framework are suggested because firebugs look for associates and the objective are to optimize a fitness value; fit bugs need to be related to high fitness parameters [12]. Let $fbug[a, :, :]$ be the D by T_F matrix with columns representing the locations of female bugs. The matrix update equation that follows is suggested for the simultaneous updating of all female insects in a specific colony employing productive Hadamard operations involving multiplication [13].

$$G_X \leftarrow repmat(Gbug(a).x, 1, T_F \quad (5) \qquad G_y \leftarrow repmat(Gbug(b).x, 1, T_F \quad (6)$$

where 'a' is an arbitrary number in the range of 1 andT_F . Repmat (P, g, n) yields an mp by nq matrix if P is a by b matrix.

$$fbug[a, :, :] \leftarrow fbug[a, :, :] + \gamma 1 \odot (G_X - fbug[a, :, :]) + \gamma 2(G_y - (G_X - fbug[a, :, :]) \quad (7)$$

It was found that the FSO method executed considerably better when $\gamma 2$ was kept lower than $\gamma 1$. Exploration is made possible by female bugs' desire to random males. Since there is less convergence of all female bugs to the position of the prevailing male, the range of answers is improved [14]. To move male bugs in the direction of the fit female bug, a particular update rule is suggested.

$$Gbug(a) \leftarrow Gbug(a) + \gamma 3 \odot (globe - Gbug(a)) \quad (8)$$

Instead of dispersing, the swarm's constituent users move as a single accumulation. As a result, every bug has to mimic the motion of other bugs. As a model of collective unity, equation (9) is put forth, in which every male bug copies the direction in which an arbitrary male bug moves towards the position of the most suitable female bug.

$$Gbug(a) \leftarrow Gbug(a) + \gamma 4 \odot (globe - Gbug(b)) \quad (9)$$

In order to avoid converge prematurely to a regional minimum, a male bug mimics the path of movement of another male bug towards the best approach rather than just moving in that direction [15].

4.PROPOSED HYBRID FSO-SVM METHOD

AI is a revolutionary technology that allows robots to learn from their observations rather than relying solely on direct programming with the help of a range of algorithms. AI can adapt within constantly changing systems without the need for complicated formulas for computation or ongoing intervention from humans [16]. Using AI techniques to enhance IoT security has come a long way in the last few years. AI methods are able to accurately understand and stop a range of IoT attacks early on by closely reviewing equipment behaviour. Furthermore, AI algorithms which fall into two primary categories offer customized options suitable for low-resource IoT devices: AI methods and ML based strategies for improving IoT security.

Biometrics has largely replaced passwords and PINs in mobile device, instrument login, accessibility limitations, and other app contexts. These days, web-based applications use it to enhance the security and efficiency of the authentication procedure. The suggested framework is based on the

fingerprint authentication system shown in Figure 1. By eliminating small features, the challenging task of identifying fingerprints is reduced to a point pattern matching problem. Minute point characteristics and their corresponding orientation mappings possess a unique durability among the different fingerprint attributes that enables them to accurately differentiate between fingerprints. Figure 2 shows the presented combined method built on data privacy and Figure 3 shows the proposed hybrid method based on attack detection [17]. Once the details are extracted, a FSO based SVM is used to identify the system attacks. In an attempt to select the best collaborators, firebugs use an optimization procedure to search within their surroundings for possible partners. The intricacy of firebug behaviour makes it imperative to identify the specific elements that pertain to the search procedure.

4.1 Authentication and access control

Before gaining access to the network, individuals and IoT devices must authenticate. IoT devices and confidential data are kept out of the hands of unauthorized users through password-based, dual-factor, and biometric identification. To control user and device access based on roles and advantages, access management procedures must be put into place.

Deliberate disruptions of the data exchange within the IoT network may also be neglected for some of the dangers that have been discovered. The gateway, also known as the sink node, which links the Internet of Things network (IoT) to the outside world, has the ability to prevent harmful threats from operating on the network by enforcing a set of rules that allow or prohibit connections. In this instance, only authorized users are allowed access to the network [18].

4.2 Intrusion detection system

Real-time detection and response to cyber threats is facilitated by ID system. These programs scan network traffic for indications of malicious or unauthorized activity. When an anomaly is detected, the IDPS can consequently launch a response, block wary traffic, or issue an alert.

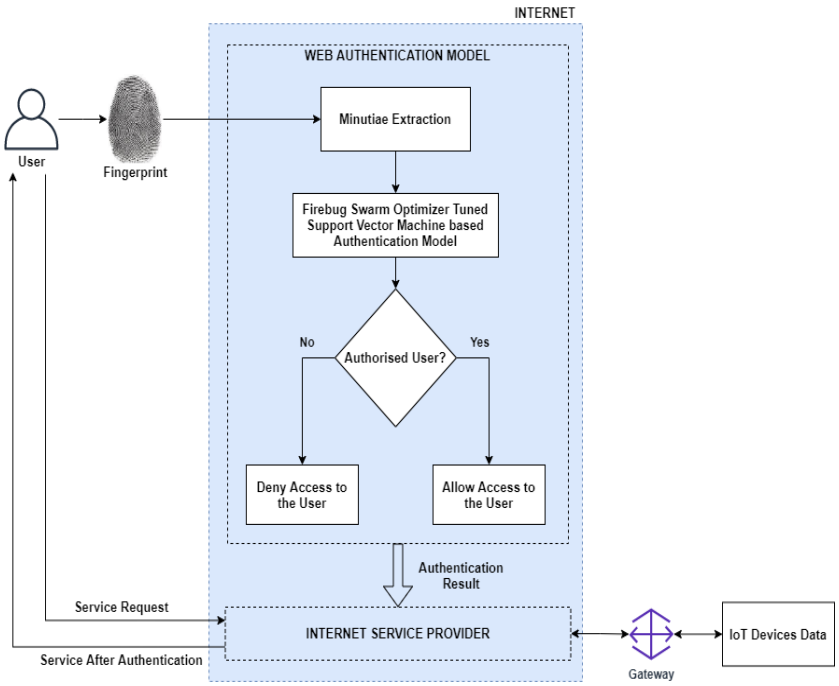

Figure 1: Proposed hybrid method based on Access Control and Authentication representation

4.3 Security audits and tracking

To detect weaknesses and safety hazards, IoT systems require routine security reviews and checks. While constant surveillance keeps an eye out for potentially malicious or suspicious activity in

system operations, network communication and behaviour from users, security reviews assess the system's security.

4.4 Privacy preserving based IoT system

Separate privacy provides statistical assurances for safeguarding personal privacy while enabling valuable analysis of information. In order to reduce the impact of individual data, unpredictability is added to the data prior to collection. This approach makes it impossible to collect data by itself while still enabling insightful analysis of aggregated data [19].

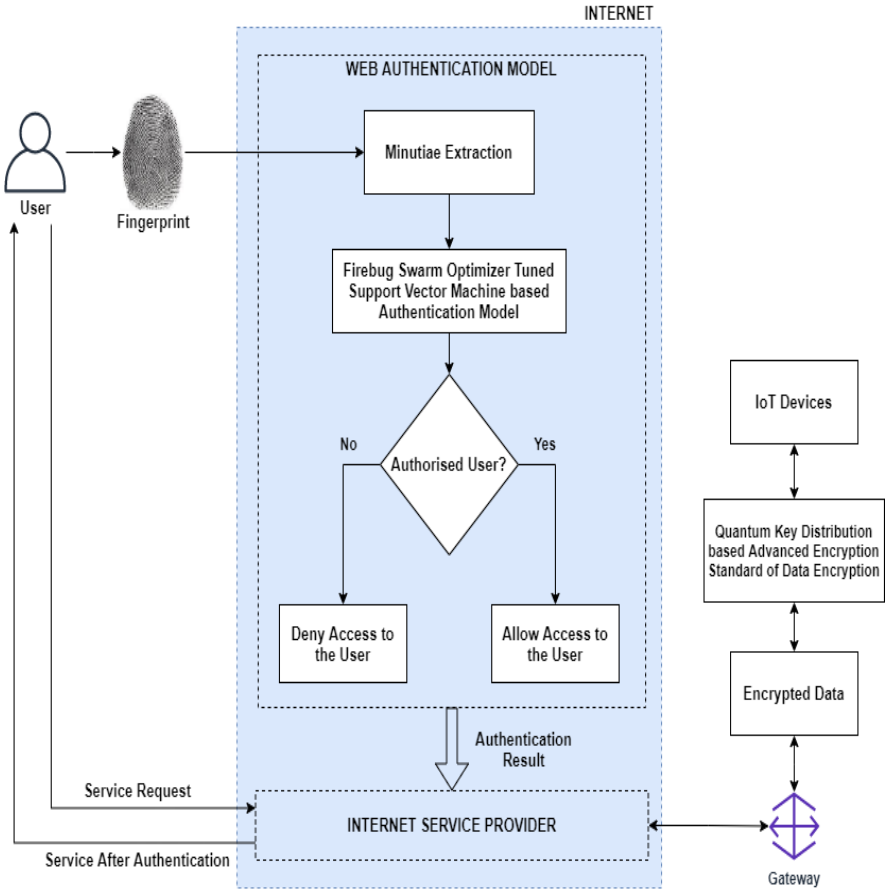

Figure 2: Proposed hybrid method based on data privacy

Quantum key distribution, the cornerstone of quantum physics, is used in our proposed approach to protect data privacy while maintaining end-to-end security over time figure 2. After enhanced encryption standards based on quantum key distribution are implemented, the authorized user can obtain access to privacy-protected data.

The use of FSOA in conjunction with the SVM classifier to increase performance is analyzed. A binary FSOA is provided for feature selection in order to achieve this performance. Additionally, a fitness function is taken into account when choosing important features and classification accuracy.

There are a lot of issues with optimization in a distinct search space. Independent solutions are needed, for example, for issues in network structure, time management theory, routing techniques, and greatest potential. A discrete model must be designed in order to carry out choice of features as shown in Figure 3. The transition from zero to one is probabilistically accomplished and is controlled by a function called a sigmoid. The FSO was driven by the same methodology is as follows:

$$P_{fbug}(a, 2{:}\,dim, n) \leftarrow \gamma 1 \odot G_x - fbug((a, 2{:}\,dim, n)) + \gamma 2 \odot G_y - fbug((a, 2{:}\,dim, n))$$

$$P_{fbug}(a, 2{:}\,dim, n) \leftarrow \gamma 3 \odot globe - Gbug((a, 2{:}\,dim, n)) \qquad (10)$$

The values of P and γ are indicated by the first two dimensions, respectively. For a given male and female bug (a,n), the values of $fbug((a,2:dim,n)$ and $Gbug((a,2:dim,n)$are set to integers in {0, 1}.

$$dimensiional = 2 + no.of\ real\ features \quad (11)$$

$Q_{P_{fbug}} > randn$ then $fbug((a,2:dim,n) = 1$ else

$$fbug((a,2:dim,n) = 0 \quad (12)$$

4.5 Calculation of fitness function

Two performance metrics that are commonly used to build a objective function are the number of features that have been selected and the accuracy of the classification. As a result, a small number of carefully chosen features and high accuracy are equivalent to a high fitness. This problem is essentially a multi-criteria decision-making task, wherein the two objectives are combined for creating a single fitness function [20]. The definition of the fitness function can be expresses as,

$$fit = Acc + (1-\eta)[1 - \frac{no.of\ features\ selected}{total\ features}] \quad (13)$$

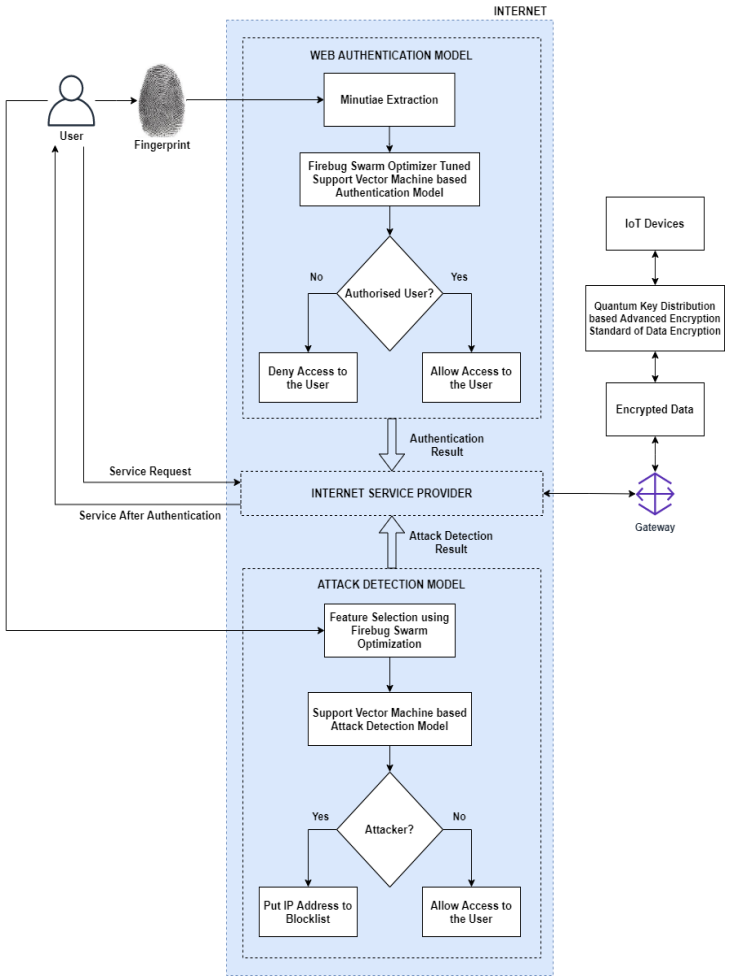

Figure 3: Proposed Hybrid Method based on Attack Detection

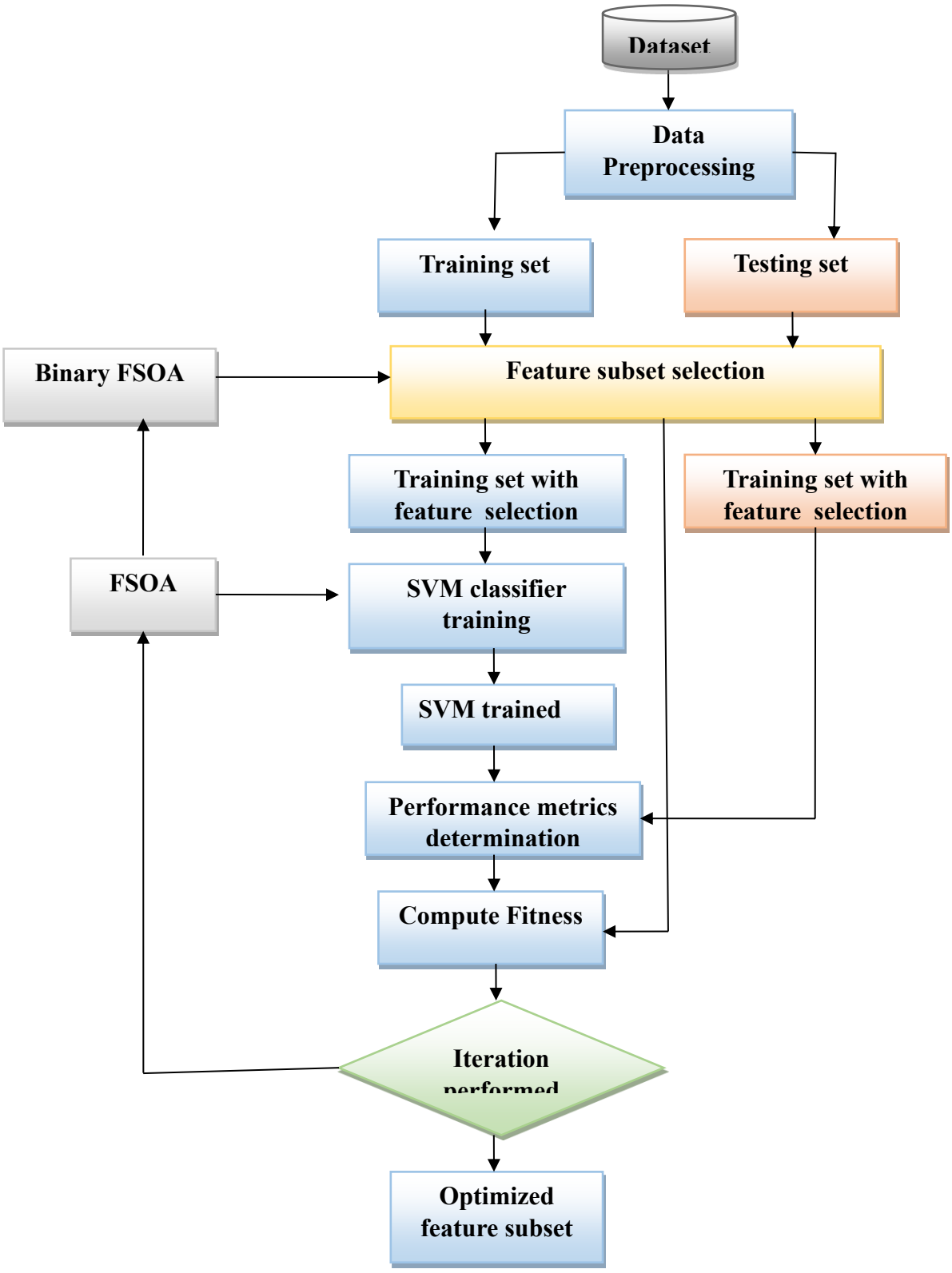

Figure 4: Flowchart of proposed hybrid FSO-SVM model

The most popular metric for assessing classifiers is accuracy, which shows the proportion of correctly classified predictions.

$$\text{Accuracy} = \frac{\text{true positive+true negative}}{\text{false positive+false negative+true positive+true negative}} \times 100\% \qquad (14)$$

$$\text{Precision} = \frac{\text{true positive}}{\text{true positive+false positive}} \times 100\% \quad (15)$$

$$\text{Recall} = \frac{\text{true positive}}{\text{true positive+false negative}} \times 100\% \quad (16)$$

$$\text{F1score} = 2 \times \frac{precision \times Recall}{Precision + Recall} \quad (17)$$

5 Proposed Hybrid FSO-SVM Algorithm

Step 1: The datasets are subjected to min–max scaling for reducing inaccuracies also to increase the efficiency of dataset connection. Additionally helpful, min-max scaling decreases numerical problems in calculations. Minimum–Maximum method used to scale the features in the intervals of [0, 1] is represented as,

$$J = \frac{\acute{J} - K}{M - K} \quad (18)$$

Step 2: Create the initial population, which includes Tm, Tf female bugs. These female bugs are spread out evenly throughout the exploration space as a vector of uniform unknowns, and the locations of every female bug within a given male bug colony are saved in an identical matrix that is updated concurrently.

Step 3: Utilize the evaluation dataset in conjunction with the proposed classifier on the training dataset. The proposed algorithm works by having each and every male bug moves in the same direction and in the orientation of a randomly chosen female bug that is the highest fit.

Step 4: The number of features that are chosen will be defined in the distinct portion of the method, and each solution's fitness value is assessed using the assigned fitness function.

Step 5: When the desired number of iterations is reached, the algorithm stops; if not, step 3 is reached.

6 RESULTS AND DISCUSSION:

This section examines the hybrid AI based on security and privacy protection method and verified with reference to the combined mathematical results for the proposed model that are employed in various usage that operate in real time. Table.1 listed the proposed hybrid model simulation parameters.

Table.1: Proposed hybrid FSO-SVM simulation parameters

Method	Parameters	Values
FSO	Iteration	30
	Female bugs	7
	Male bugs	20
	$\gamma 1$	-0.75x rand (Dim, Tf)
	$\gamma 2$	0.75x rand (Dim, Tm)
	$\gamma 3$	1.5x rand (Dim)
	$\gamma 4$	0.75x rand (Dim)
SVM	Population number	100
	Penalty parameter	Variable

Table.2: Performance comparison for various classification models

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)
LeNet -5	88.9	90.5	80.9	78.9
ResNet -50	87.4	85.0	88.9	86.5
ResNet-101	86.5	82.3	89.6	87.4
ResNet-152	92.2	89.1	91.4	89.7
Hybrid (proposed)	99.1	99.0	98.7	98.8

Table.2 provides the performance comparison of various models such as LeNet-5, ResNet -50, ResNet-101, ResNet-152 and proposed hybrid model taken into consideration. Here, performance metrics such as, accuracy, precision, recall and F1-score were determined. From table, the existing LeNet model obtained the performance value of 88.9%, 90.5%, 80.9% and 78.9% respectively. The existing ResNet-50 model obtained the performance metrics of 87.4%, 85%, 88.9% and 86.5% respectively. The existing ResNet-101 model obtained the performance value of 86.5%, 82.3%, 89.6% and 87.4% respectively. The existing ResNet-152 model obtained the values of 92.2%, 89.1%, 91.4% and 89.7% respectively. The proposed hybrid algorithm obtained the accuracy, precision, recall and F1-score value of 99.1%, 99%, 98.7% and 98.8% respectively. By analyzing the results the proposed model gives better performance metrics.

Two different groups were created from the 5100 data collection procedures that comprised the dataset: training dataset (80%) and testing data (20%). Only the training dataset was readily misidentified with the testing datasets. FSO-SVM attained the highest levels of precision and accuracy, at roughly 99% and 100%, respectively FSO-SVM also achieved the highest F1 scores with 99.5%. ResNet-101 had the best recall score, which was 98.7%.

The mean of precision and recall are compared for various precision evaluation metrics in Figure 5. Choosing to use a particular variable to draw inferences is necessary because the reliability of the model cannot be stated clearly. As security grows, the model's resilience will rise because it will be more resistant to content attacks. Conversely, the one with a lower value will be perceived as operating at a lower level. By analysing the precision results the proposed hybrid model gives better performance metric than the existing LeNet-5, ResNet models.

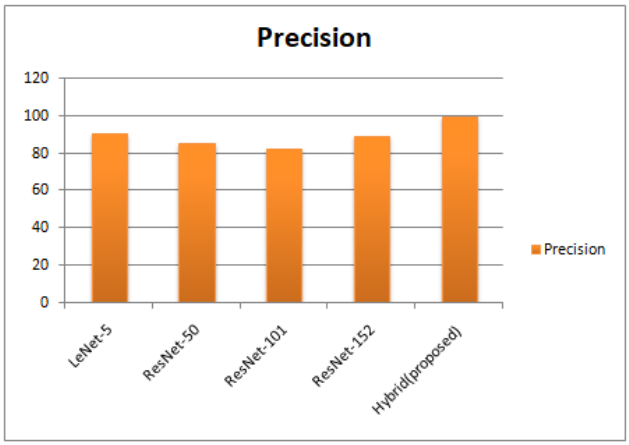

Figure 5: Performance graph of precision for proposed model and existing model

A statistical indicator of binary models' accuracy that is used to assess the accuracy of unstable data is recall value. It considers the classification algorithm's recall and accuracy rates as well. Model accuracy and recall rates can be ranked to calculate recall. Additionally, the indicator used in Figure 6: comparison for various recall assessment indicators quantifies the model's overall performance which is significantly higher than that of other types of networks currently in use.

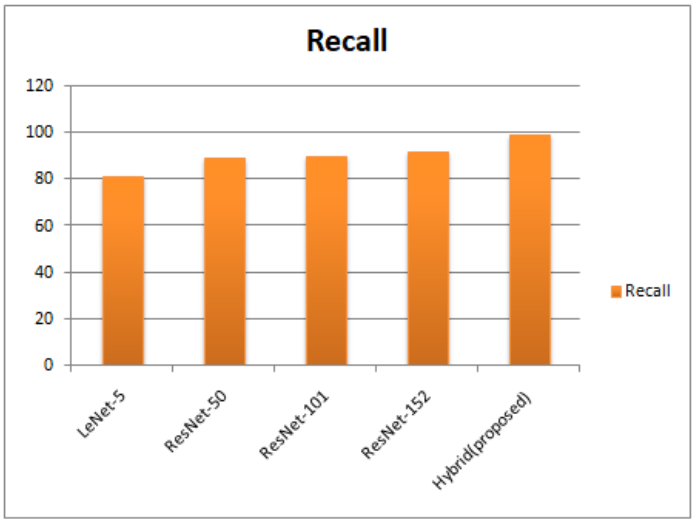

Figure 6: Performance graph of recall for proposed model and existing model

The performance of ResNet-152 and ResNet-5 is comparable. Remember that ResNet can perform better than other parameters and, therefore, could work well in a variety of situations. ResNet-50 and ResNet-101 are the least accurate ResNet models.

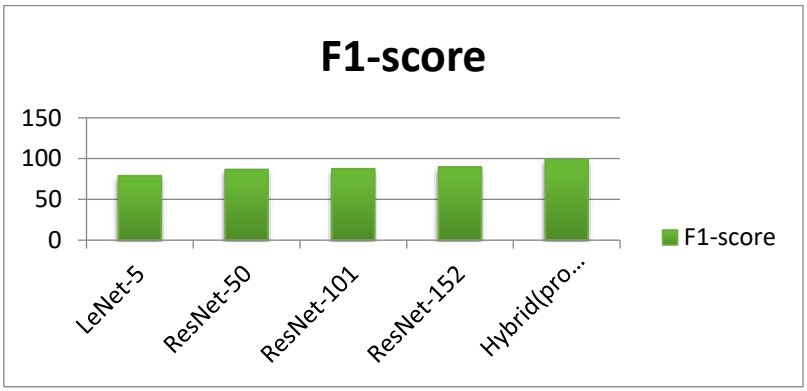

Figure 7: Performance graph of F1-score for proposed model and existing model

The FSO-SVM accomplished better than the other models because the dense blocks could reuse features. In the performance metrics presented in Figure 7 for the applied CNN Models of F1-score, FSO-SVM models outperform the competition with respect to feature performance.

Figure 8 shows the performance comparison of accuracy of proposed method and existing techniques. Based on the results the proposed method achieved better accuracy.

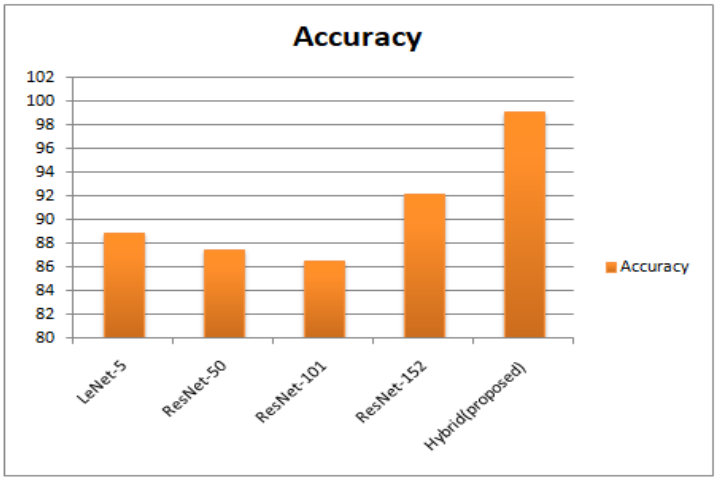

Figure 8: Performance graph of accuracy for proposed model and existing model

Figure 9 shows the Graphical representation of proposed method performance results. Here, provides the performance comparison of various models such as LeNet-5, ResNet-50, ResNet-101, ResNet-152 and Hybrid based CNN model taken into consideration. The performance metrics such as, accuracy, precision, recall and F1-score were determined.

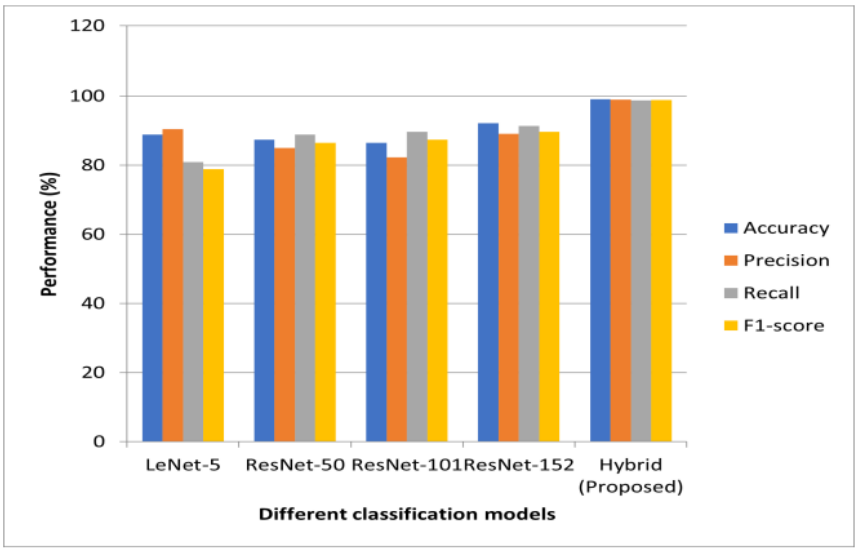

Figure 9: Graphical Representation of Proposed Hybrid Method Performance Results

7. CONCLUSION:

The term Internet of Things describes a situation in which an extensive array of interconnected and diverse devices (often referred to as things) communicate with each other regardless of time or location. This enables objects to establish social connections with one another based on predetermined rules established by their owner. The proposed model is free from many attacks or malicious traffic. Only the authorized user can access the network and data. The methodology is scalable, reliable and more accurate so that applicable to Social IoT with large number of nodes. Automated computer calculation can be done so calculation complexity and time consumption can be minimized which leads to low energy consumption. So, the proposed framework is more accurate and precise.

REFERENCES:

[1] Nobakht, M., Sivaraman, V., & Boreli, R. (2016, August). A host-based intrusion detection and mitigation framework for smart home IoT using OpenFlow.

[2] 11th International conference on availability, reliability and security (ARES) (pp. 147-156). IEEE.

[3] Atzori, L., Iera, A., Morabito, G., & Nitti, M. (2012). The social internet of things (siot)–when social networks meet the internet of things: Concept, architecture and network characterization. Computer networks, 56(16), 3594-3608.

[4] Michalski, R. S., Carbonell, J. G., & Mitchell, T. M. (Eds.). (2013). Machine learning: An artificial intelligence approach. Springer Science & Business Media.

[5] Senthil Kumar, J., Sivasankar, G., &SelvaNidhyananthan, S. (2020). An artificial intelligence approach for enhancing trust between social IoT devices in a network. In Toward Social Internet of Things (SIoT): Enabling Technologies, Architectures and Applications (pp. 183-196). Springer, Cham.

[6] Punithavathi, P., Geetha, S., Karuppiah, M., Islam, S. H., Hassan, M. M., &Choo, K. K. R. (2019). A lightweight machine learning-based authentication framework for smart IoT devices. Information Sciences, 484, 255-268.

[7] Newaz, A. I., Sikder, A. K., Rahman, M. A., & Uluagac, A. S. (2019,October). Healthguard: A machine learning-based security framework for smart healthcare systems. In 2019 Sixth International Conference on Social Networks Analysis, Management and Security (SNAMS) (pp. 389-396). IEEE.

[8] Wang, B., Sun, Y., Duong, T. Q., Nguyen, L. D., & Zhao, N. (2020). “Security enhanced content sharing in social IoT: A directed hypergraph-based learning scheme. IEEE Transactions on Vehicular Technology, 69(4), 4412-4425.

[9] Ullah, F., Naeem, M. R., Mostarda, L., & Shah, S. A. (2021). Clone detection in 5Genabled social IoT system using graph semantics and deep learning model. International Journal of Machine Learning and Cybernetics, 12(11), 3115- 3127.

[10] Karthik, E., &Sethukarasi, T. (2022).Sarcastic user behavior classification and prediction from social media data using firebug swarm optimization-based long short term memory. The Journal of Supercomputing, 78(4), 5333-5357.

[11] Divya., N. J., R. Kanniga Devi, and M. Muthukannan., (2024), Privacy-AwareIoT-Based Multi-Disease Diagnosis Model for Healthcare System, *Computer Vision and AI-Integrated IoT Technologies in the Medical Ecosystem* ,376-406.

[12] Pérez Arteaga., Sandra., Ana Lucila Sandoval Orozco, and Luis Javier GarcíaVillalba.,(2023), Analysis of machine learning techniques for information classification in mobile applications, *Applied Sciences* 13(9)5438.

[13] Le., Tan, and Sachin Shetty.,(2022), Artificial intelligence-aided privacy -preserving trustworthy computation and communication in 5G-based IoT networks." *Ad Hoc Networks* 126,102752.

[14] Alzubi., Omar A., Jafar A. Alzubi., K. Shankar., and Deepak Gupta., (2021),Blockchain and artificial intelligence enabled privacy-preserving medical data transmission in Internet of Things, *Transactions on Emerging Telecommunications Technologies* 32(12),e4360.

[15] Hennebelle., Alain., Leila Ismail., HunedMaterwala., Juma Al Kaabi., Priya Ranjan, and Rajiv Janardhanan.,(2024), Secure and privacy-preserving automated machine learning operations into end-to-end integrated IoT-edge-artificial intelligence-blockchain monitoring system for diabetes mellitus prediction." *Computational and Structural Biotechnology Journal* 23,212-233.

[16] Khalid., Nazish., Adnan Qayyum., Muhammad Bilal., Ala Al-Fuqaha, and JunaidQadir.,(2023), Privacy-preserving artificial intelligence in healthcare: Techniques and applications,*Computers in Biology and Medicine* 158,106848.

[17] Selvarajan., Shitharth., Gautam Srivastava., Alaa O. Khadidos., Adil O. Khadidos., Mohamed Baza., Ali Alshehri, and Jerry Chun-Wei Lin.,(2023), An artificial intelligence lightweight blockchain security model for security and privacy in IIoT systems, *Journal of Cloud Computing* 12(1),38.

[18] Chikkalwar.,Sudha Rani, and YugandharGarapati.,(2023), Network intrusion detection system using bacterial foraging optimization with random forest." *International Journal of Advanced Technology and Engineering Exploration* 10(105),1037.

[19] Christiana Ionone, Vasos Vassiliou. "Network Attack Classification in IoT Using Support Vector Machines", Journal of Sensor and Actuator Networks, 2021

[20] Khademolqorani., Shakiba, and ElhamZafarani.,(2024), A novel hybrid support vector machine with firebug swarm optimization, *International Journal of Data Science and Analytics* ,1-15.

[21] Alabdulhafith., Maali., SalwaOthmen., AymanAlfahid., ChahiraLhioui., Ghulam Abbas., Rim Hamdaoui., Wael Mobarak, and Yasser Aboelmagd.,(2024),Implementing a Transfer Learning For User Behavior Analysis and Prediction using Preference-dependent Model, *IEEE Access*.