International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Soft computing based Machine Learning Enhancement Approach for Privacy and Security in Macro Layer IoT Devices Using Cyber Security Techniques

Ebenezer V Roselin[1] , Victor. S. P[2]

Submitted: 25/02/2023 **Revised:** 15/04/2023 **Accepted:** 05/05/2023

Abstract: The communication and access domination of IoT devices from human to machine or machine to human are one way controllable through user or administrator in the entire communication system with easier manner but it is entirely different on machine to machine communicating IoT devices. The timing of data communication may be unknown for the user/administrator in machine to machine focused IoT devices and more number of cases with wireless mode than with the wired mode. The process of collecting the data, ordering the data, and checks for privacy and security issues in a machine to machine IoT device is a complex process to implement. The existing methodologies focus on the IoT device connection management to the network and verify the communication among several network devices either in local server or to a remote server. This research article proposes anoptimistic machine learning enhancement approach for privacy and security in macro layer IoT devices using cyber security techniques. In future this research paper will be extended with the implementation ofautomated privacy and security module towards all the major layers of IoT devices such as micro, mini and macro layer IoT devices.

Keywords*: Machine learning, IoT, Cyber security, Macro layer, Privacy data*

I. Introduction:

M2M(Machine to Machine) vs. IoT devices:

IoT (Internet of Things) refers to the interconnectivity of physical devices and objects embedded with sensors, software, and network connectivity, allowing them to collect and exchange data. M2M (Machine to Machine) communication refers to direct communication between devices without human involvement.

Both IoT and M2M are related concepts and overlap in many aspects, but the main difference is that IoT encompasses a larger system that involves not only machine communication but also human interaction with the devices and data.

1Research Scholar, Manonmaniam Sundaranar University, Tirunelveli
Email: ebiroselin@gmail.com
2Associate Professor, Department of Computer Science, St. Xavier's College, Tirunelveli
drspvictor@gmail.com

Privacy data:

The right of privacy is a fundamental right. It is a right which protects the inner sphere of the individual from interference from both State, and non-State actors and allows the individuals to make autonomous life choices.It refers to the protection of personal information and ensuring that it is not misused or accessed without authorization.

One example of data privacy is ensuring that sensitive data, such as financial information or medical records, is only accessed by authorized personnel.

Machine Learning:

Machine Learning is the field of study that gives computers the capability to learn without being explicitly programmed. This amazing technology helps computer systems learn and improve from experience by developing computer programs that can automatically access data and perform tasks via predictions and detections.

II. Methodology

The proposed methodology contains five stages for the soft computing based machine learning enhancement approach for privacy and security in macro layer IoT devices using cyber security techniques. They are,

Stage-1: Examine Macro layer IoT devices

a. Set Base layer=Mini layer

- Identify and filter the macro layer IoT device from the IoT resources.

b. List the Macro Layer IoT devices.

c. Macro layer IoT device architecture.

d. Macro Layer IoT device data and communication.

Stage-2: Identify the Issues related to privacy and security

a. Mild priority

b. Moderate priority

c. Elevated priority

d. Severe priority

e. Extreme priority

Stage-3: Handle the issues using soft computing techniques based machine learning

a.Theory of automata

b.Fuzzy logic

c.Neural networks

d. Genetic algorithm

e. Artificial intelligence

Stage-4: Cyber security based privacy and security maintenance

a. Interoperability - Admin Cyber security –Authentication/authorization

b. Encryption standards-DES, AES, Elliptic curve cryptography

c. Standard Communication modes- Auth2.0, TLS, SSL

d. Tamper resistant Mechanism-smart cards

e. Secure Trusted Execution Element-Smart card

Stage-5: Testing

Testing tools for macro IoT devices privacy and security management

- ❖ Open source testing tool for attacks

The proposed methodology of soft computing based machine learning enhancement approach for privacy and security in macro layer IoT devices using cyber security techniquesis as follows in Fig-1.

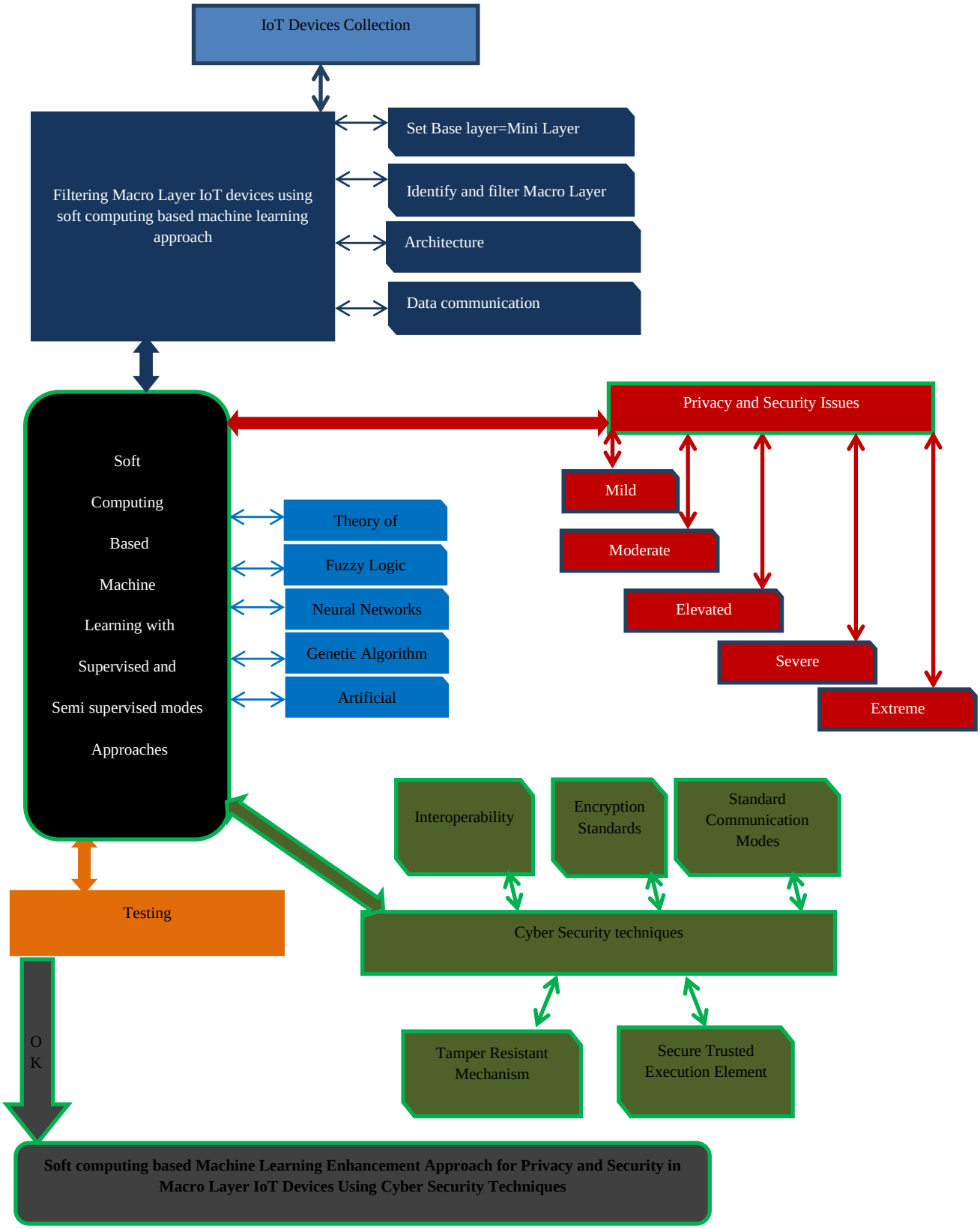

Fig-1: Proposed Soft computing approach for IoT privacy and security

The algorithm for the soft computing based machine learning enhancement approach for privacy and security in macro layer IoT devices using cyber security techniques is as follows,

Start

Input: IoT devices collection with information

Step-1: Examine macro layer IoT device

a. Identify the macro layer IoT device from the IoT resources.

b. List the Macro Layer IoT devices.

c. Macro layer IoT device network architecture.

d. Macro Layer IoT device data and communication.

Step-2:Identify the Issues related to privacy and security

a. Mild priority

b. Moderate priority

c. Elevated priority

d. Severe priority

e. Extreme priority

Step-3: Handle the issues using Soft computing based Machine learning approaches

a. Theory of automata with supervised learning mode.

b. Fuzzy logic with supervised learning mode.

c. Neural networks with supervised learning mode.

d. Genetic algorithmwith semi supervised learning mode.

e. Artificial intelligence with semi supervised learning mode.

Step-4:Cyber security based privacy and security maintenance

a. Interoperability

b. Encryption standards

c. Standard Communication modes

d. Tamper resistant Mechanism

e. Secure Trusted Execution Element

Step-5: Testing

Test results are ok; Break; if all the above are success go to end

Else goto step-1; End if;

End;

III. Implementation

Stage-1: Filter the Macro layer IoT devices

a. Identify and filter the macro layer IoT device from the IoT resources.

Set Base layer=Mini layer

The IoT devices in which the access of IoT device dominated by Machine to Machine then the particular devices are categorized as Macro Layer IoT devices.

b. List the Macro Layer IoT devices.

i. Smart Water meter.
ii. Smart Electricity meter.
iii. Smart Vehicle console (Speed, fuel, GPS, distance to cover)
iv. Automated supply chain management.
v. ATM machines.
vi. Smart vending machine etc.

c. Architecture (Network).

The machine learning based IoT working mechanism is as follows in fig-2:

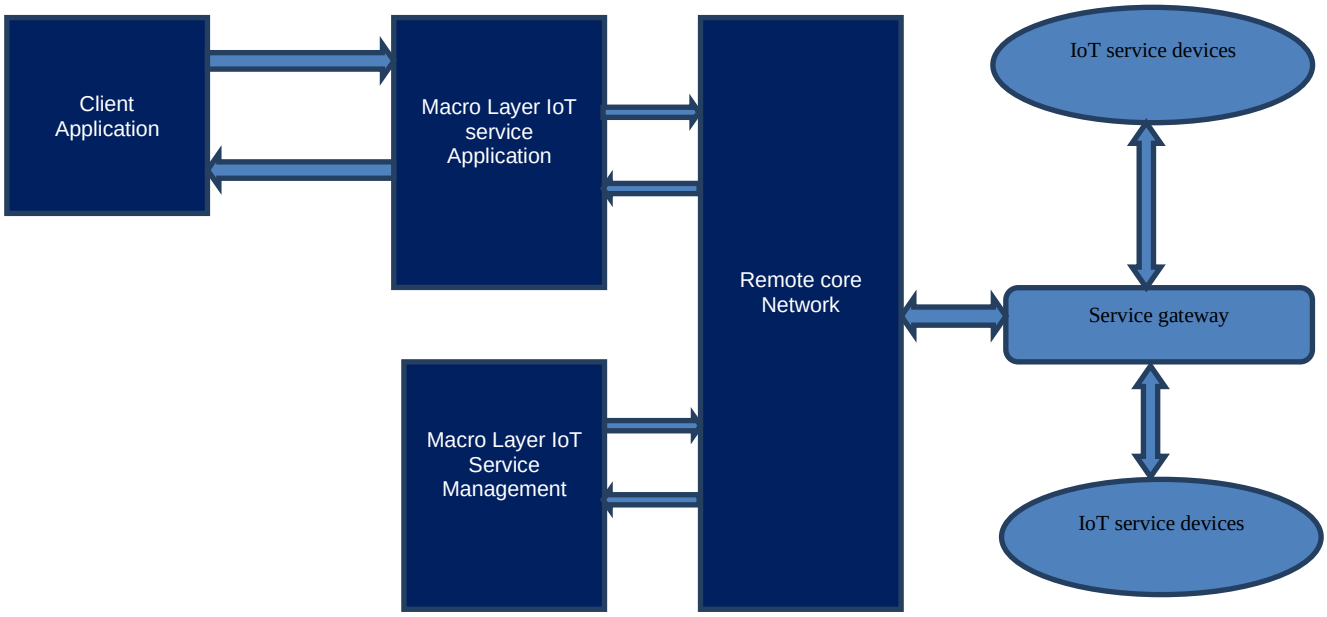

Fig-2: Macro layer IoTnetwork architecture

d. Data and communication.

The communication modes used for data transfer in Macro IoT devices includes the following options:

- Wired (single PC/LAN)
- Cellular(GSM-2G/UMTS-3G/LTE-4G/5G)
- Wi-Fi(2.4G/5G)
- Bluetooth(4.0,5.0 A2DP)
- Satellite

Stage-2: Identify the Issues related to privacy and security

a. Mild priority

i. Stolen Passwords (external)

The unauthorized users access the Macro IoT devices with the stolen passwords through keyboard loggers lead to the entire system privacy and security breach with a negative impact. The basic attack is on the profile data for seeking further access rights.

ii. Unauthorized access (internal)

Every user have their own access rights if the process of attacking an IoT device through other high profile rights which are not permitted will affect the privacy and security data in a network. The internal devices connected to the network try to access the other IoT devices or components data.

b. Moderate priority

i. Trojan horse (Unauthorized device injection)

The process of injecting an unauthorized device infiltrated into the macro IoT device network harm the privacy and security of the current network profile environment. Unknown devices found in the network connected devices list are the primary signs of the Trojan horses which may not be genuine.

ii. Connection interruption

The process of disrupting the communication among macro IoT devices affects the security ofeffective data communication through data loss and data corruption. Without proper security patches the connection interruption increases the security of the device moderately.

c. Elevated priority

i. Interception

Hackers use the IoT devices to access data communication and control the user's network devices, daily routines and setting up privacy data leaks. The privacy data is entire leaked or observed confidentially to affect the security of the system in near future.

ii. DDoS attack
The distributed denial of service attacks disrupts the normal functioning of the macro IoT networks by blocking the service mechanism within the network. Accessing any particular services are in denied state lead to the entire functionality failure for data communication.

d. Severe priority

i. Man in the middle
Altering the information on macro IoT devices the hackers misuse the network profile and control the user's network devices, daily routines and setting up friends and foes. The modification of information affects the entire communication security in any affected network.

ii. Ransom ware
Hijacking the macro IoT device data for monetary benefits affect the entire organization in the area of privacy and security concern. The data with lot of privacy information are hijacked , the functionality of the current system will be affected along with the threat to the security of all the devices connected in the entire network will also be ready to face the attack.

e. Extreme priority

i. Failed service/ Halting/Un expected behavior
Macro IoT devices are unable get the services/updates by tampering the network profile and affect its security.
In order to reduce certain brand values, thehackers attack the IoT devices through vulnerability holes in the network profile.

The entire functionality of the macro IoT device attains halted state/unexpected behavior of outcomes due to the hacking operation. Some hackers attack smart printers to print something remotely in order to insist their opinion globally.

Stage-3: Handle the issues using Soft computing based Machine learning techniques
a. Theory of automata
Automata theory as in fig-3 and fig-4 are used to deal with mild level privacy and security issues.
i. Stolen passwords

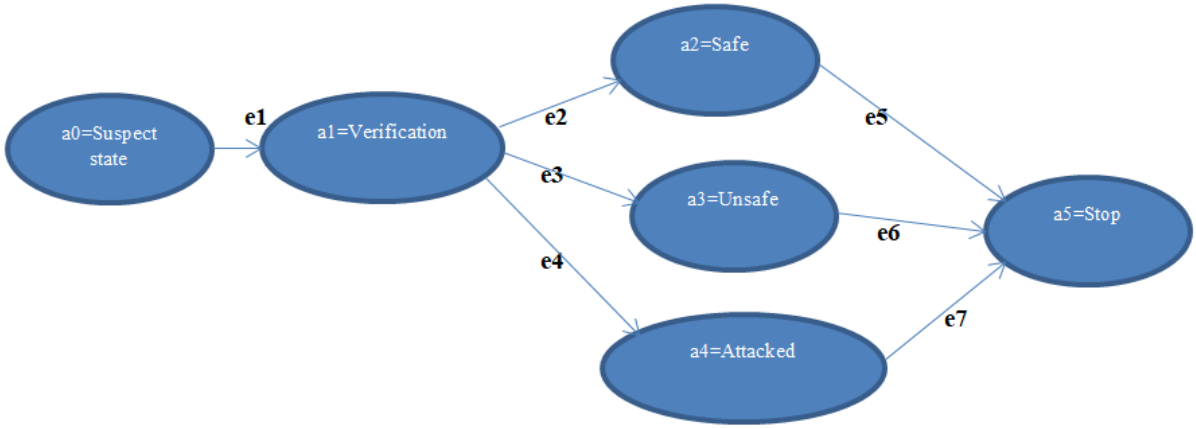

Fig-3: Automata theory based mild level privacy and security issue handling-1
The following table-1 represents the edge functions in the automata.

Table- 1: Edge function-1 table

Sl.No	Edges	Function/operation/inputs
1	e1	Router configuration login
2	e2	Genuine logs
3	e3	Satisfied logs
4	e4	Compromised logs
5	e5	Increase Frequent monitoring
6	e6	Cyber security based password change
7	e7	Cyber security based device protection

ii. Unauthorized access

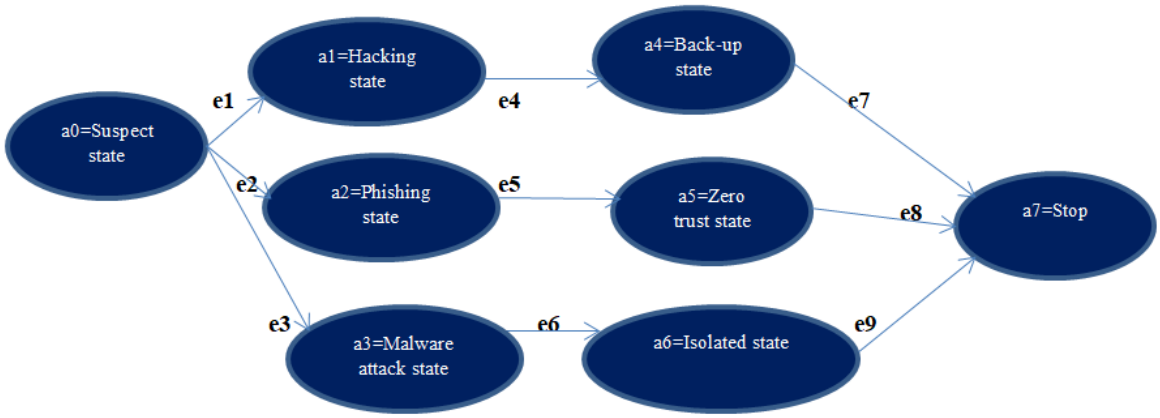

Fig-4: Automata theory based mild level privacy and security issue handling-2

The following table-2 represents the edge functions in the automata.

Table-2: Edge function-2 table

Sl.No	Edges	Function/operation/inputs
1	e1	Password authentication leak
2	e2	Policy rights leak
3	e3	Software vulnerability
4	e4	Multi factor authorization
5	e5	Implement least privilege
6	e6	Update patch and security software
7	e7	Cyber security based access protection
8	e8	Cyber security based access protection
9	e9	Cyber security based access protection

b. Fuzzy logic

Fuzzy logic based machine learning is used to deal the moderate level privacy and security issues.

i. Trojan horse (Unauthorized device injection)

The fuzzy membership value as in table-3 ensures the Trojan horse presence in the macro IoT device communication environment.

Table-3: Fuzzy membership function value for Trojan horse handling

Sl.No	Event	Fuzzy membership value	Result
1	Unexpected slower performance	0.1	Data clean
2	High data volume transfer	0.2	Network reset
3	Suspected audit	0.3	Filter genuine devices
4	Netstat-a results	0.4	Isolate unknown devices
5	Device manager results	0.5	Unplug and plug all the network devices and monitor
6	Port scan manager results	0.6	Flash port and recheck if again exists then apply cyber security techniques.
7	Endpoint detection and response (EDR)	0.7	Router configuration change and recheck if again exists then apply cyber security techniques
8	Network monitor	0.8	Cyber security technique required
9	Intrusion detection monitor	0.9	Cyber security technique required
10	Internet security software	1.0	Cyber security technique required

ii. Connection interruption

The fuzzy membership value as in table-4 ensures the connection interruption in the macro IoT device communication environment.

Table-4: Fuzzy membership function value for connection interruption handling

Sl.No	Event	Fuzzy membership value	Result
1	Internet Service Provider frequent cuts	0.1	Change IP address
2	FTTH/Mobile tower cuts	0.2	Reset FTTH port
3	Router to Internet Service provider	0.3	Reset router
4	Other IoT devices to Router	0.4	Unplug and plug all the IoT devices and monitor
5	Router to other IoT devices	0.5	Change Router configuration channels
6	Router side cuts	0.6	Change latest Router
7	Macro IoT device to Router	0.7	Cyber security technique required
8	Router to Macro IoT device	0.8	Cyber security technique required
9	Frequent interval time Router to and fro Macro IoT device	0.9	Cyber security technique required
10	Frequent long interruption time Router to and fro Macro IoT device	1.0	Cyber security technique required

c. Neural networks

The Neural network approach as in fig-5 and fig-6 are used to handle elevated level privacy and security issue of Macro IoT devices.

i. Interception

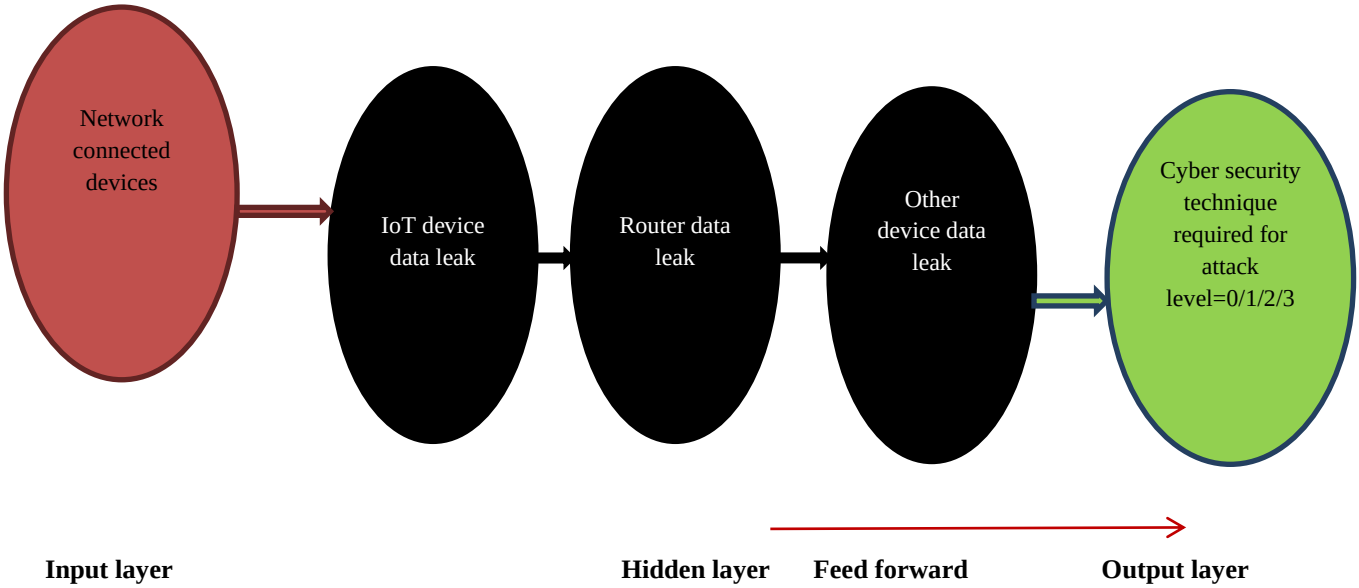

Fig-5: Neural networks for dealing interception

- Input layer=network connected devices
- Hidden layer-1=IoT device data leak
- Hidden layer-2=Router data leak
- Hidden layer-3=Other connected device data leak
- Output layer=Cyber technique required for attack level={null/monitor mode, device, modem, network}

ii. DDoS attack

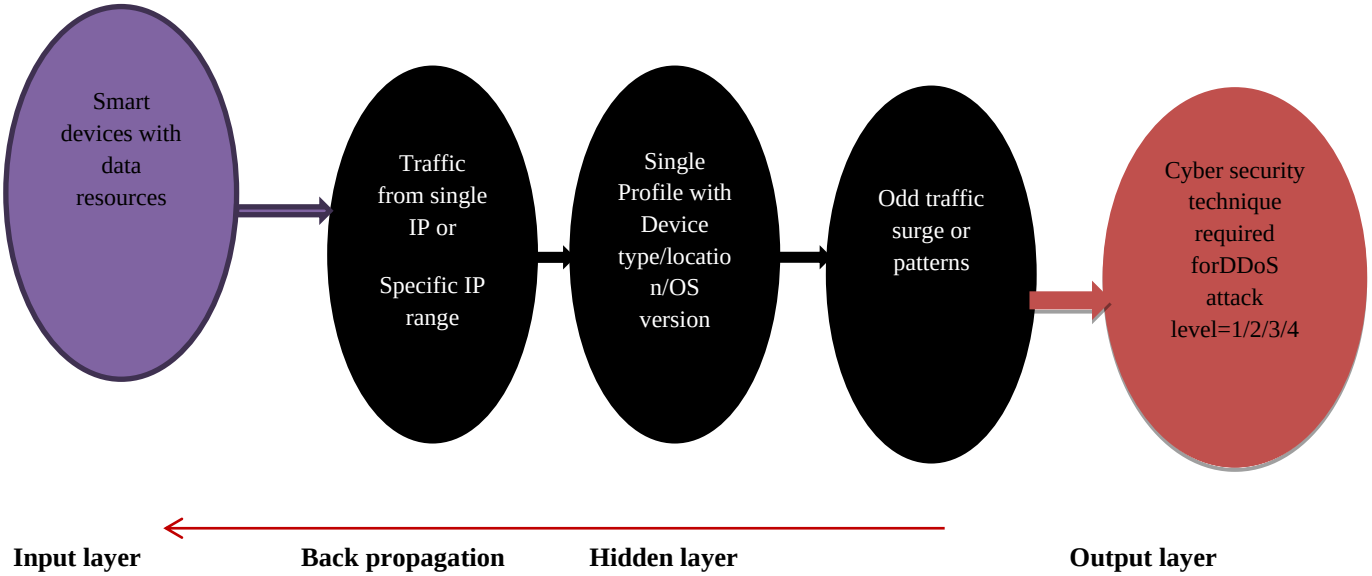

Fig-6:Neural networks for dealing DDoS attack

- Input layer=network connected devices
- Hidden layer-1=IoT device data leak
- Hidden layer-2=Router data leak
- Hidden layer-3=Other connected device data leak
- Output layer=Cyber technique required with attack level={Black hole routing, Rate limiting, Application firewall, Network diffusion}

d. Genetic Algorithm

Genetic algorithmic approach plays the vital role in solving severe level privacy and security issue of Macro IoT devices. Since the combination of crypto security algorithms are very essential to handle the severe level issues.

i. Man in the Middle Attack

The following steps are used in GA approach:

Step-1:Initialize the Macro IoT devices

Step-2: Determine the security profile, access and communication levels

Step-3: Selection of issues

- *Malware Proxy*
- *Certificate Pinning*
- *Spoofing*
- *Phishing*

Step-4: Crossover of solutions

Virtual Private Network with Advanced Transport Layer Security

Step-5: Ensure security with User and Entity Behavior Analytics (UEBA)

ii. Ransomware

The following steps are used in GA approach:

Step-1: Initialize the suspicious ransom ware affected IoT devices

Step-2: Determine the data security, validity and priority levels

Step-3: Selection of issues

- *Data Stealing Ransom ware*
- *Locker Ransom ware*
- *Double Extortion Ransom ware*
- *Triple Extortion Ransom ware*

Step-4: Crossover of solutions

Paid decryption and Recovery tools with isolation or Instant report and save the rest

Step-5: Ensure security with available back ups

e. Artificial Intelligence with deep learning

The artificial intelligence is used to deal with the extreme level privacy and security issues in macro layer IoT devices. The automated and fast responses supported by AI with deep learning are essential to handle extreme level attacks.

The following steps are used in AI with deep learning approach:

Step-1: Install AI security server with vast amount of threat information's and patterns

Step-1: Initialize the suspicious IoT devices

Step-2: Collect the suspicious activity logs and potential threat data

Step-3: Analyze the listed components

- *Network traffic*
- *User interaction*
- *System logs*
- *External threat data*

Step-4: if pattern=known

Apply cyber security technique

else

Instant network alert for unknown pattern study;

Perform mitigation action by brute force attack;

End if

Step-5: Store the newly learned pattern and solution

Stage-4: Cyber security based privacy and security maintenance

a. Interoperability

The mild level attacks are handled with interoperability cyber security technique approach.

The main focus is on Administrator level Cyber security which includes the following two components:

- *Identification*
- *Authentication*
- *Authorization*

b. Standard Communication modes

The moderate level attacks are handled with standard communication modes cyber security technique approach.

The primary target is onsecured protocols for communication which includes the following three components:

- *Auth2.0,*
- *Transport Layer Security,*
- *Secure Socket Layer.*

c. Encryption standards

The elevated level attacks are handled with encryption data standards in cyber security technique approach.

The concentration is on data encryption algorithms with less complexity which includes the following three components:

- *Data Encryption Standard(DES)*
- *Advanced Encryption Standard(AES)*
- *Elliptic Curve Cryptography(ECC)*

d. Tamper resistant Mechanism

The severe level attacks are handled with tamper resistant mechanism in cyber security technique approach. It includes 2 components

- *TPM-Trusted Platform Module-Separate module in main board*
- *TEE-Trusted Execution Environment-Incorporated within main board*

e. Secure Trusted Execution Element

The extreme level attacks are handled with secure trusted execution element in cyber security technique approach.

The cyber security module is incorporated within these elements as follows:

- *EMV chip card*
- *Smart cards*

Stage-5: Testing

Testing tools for macro IoT devices privacy and security management

The following testing tools as in fig-7 and fig-8are used for macro IoT devices privacy and security improvement using cyber security techniques.

i. Kali-Linux tool [10]

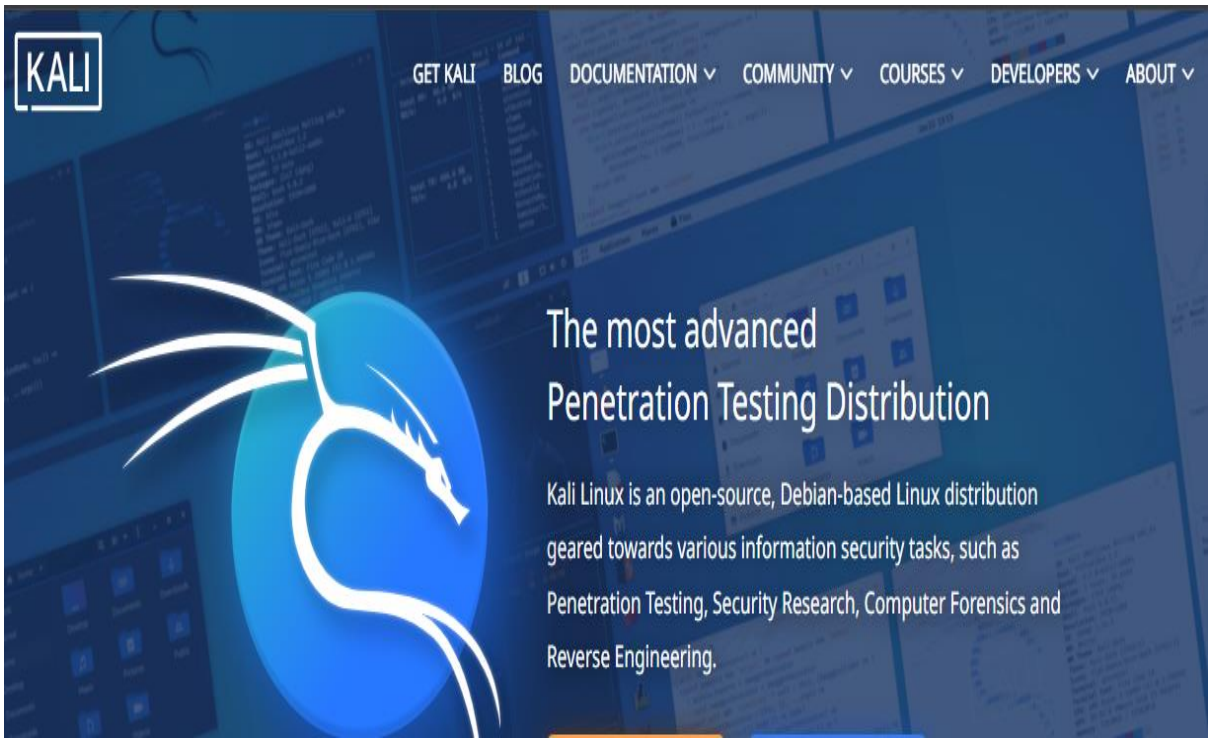

Fig-7: IoT privacy and security Testing tool-1

ii. OSSEC [11]

Fig-8: IoT privacy and security Testing tool-2

IV. Results and

Discussion

The standard datasets from Kaggle standard data set [8] and Github [9] with a collection of 15 data resources along with the real time IoT device connection such as

- Smart vehicle tracking,
- Smart pad,
- Smart watch,
- ETDS,
- E alarms
- Smart Health monitor etc.(from different brands)

The proposed methodology produces the most accurate results by applying the proposed soft computing based machine learning enhancement approach for privacy and security in macro layer IoT devices using cyber security techniques.

This research article gives 93.3% (14 out of 15 IoT data sets) of success rate for the proposed soft computing based machine learning enhancement approach for privacy and security in macro layer IoT devices using cyber security techniques.

The result comparison of existing network security approach and proposed soft computing methods with the parameters such as accuracy, precision, recall, and F1score etc. are represented in the below Table-5format,

Table-5: Proposed methodology parametric comparisons

No	Approach	Accuracy	Precision	Recall	F1 score value
1	Privacy and security management using existing network security approach using cryptography for connected devices.	53%	0.53	0.51	0.52
2	Soft computing based machine learning enhancement approach for privacy and security in macro layer IoT devices using cyber security techniques	93%	0.93	0.92	0.93

The following fig-9 shows the performance comparison between the proposed and existing methodologies.

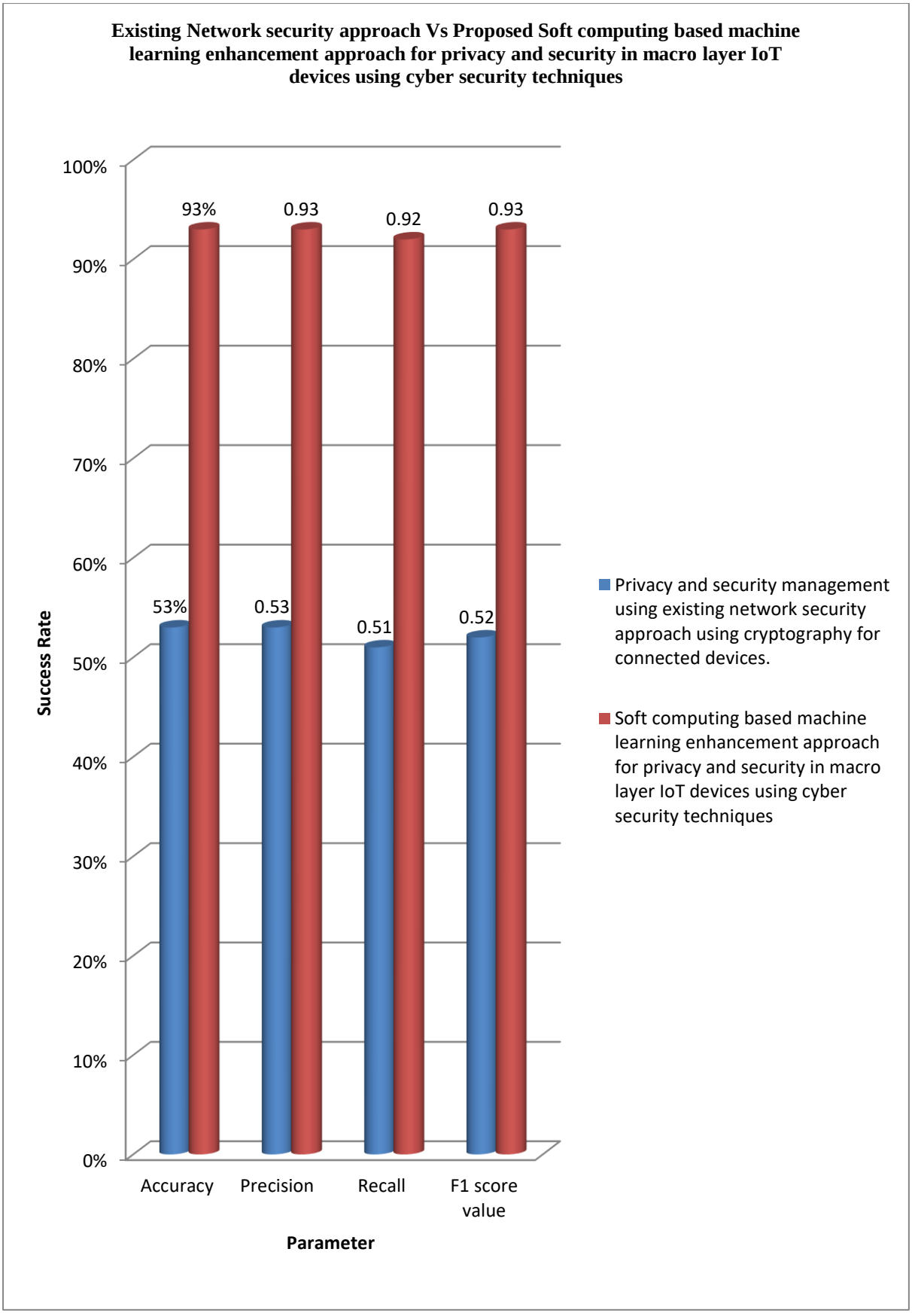

Fig-9:Proposed vs. existing methodology performance comparisons

V. Conclusion:

The macro layer IoT devices are complex when compared with the micro layer and mini layer IoT devices due to its communication dominance. The human interaction enabled M2M devices are only considered as the macro IoT devices with machine to machine communication dominance.

The new researches in the field of macro IoT are important to automate the privacy and security in IoT data transmissions due to its vast amount of information handling nature. The proposed soft computing based machine learning enhancement approach for privacy and security in macro layer IoT devices using cyber security techniquesinitially focused with the macro IoT devices filtration based on its communication dominance, then focuses on macro layer IoT devices privacy and security issues, followed by the soft computing based machine learning techniques in order to solve the privacy and security issues recognitionand then focus on to the appropriate Cyber security techniques for implementation and finally test the privacy and security efficiency.

This research article gives 93.3% (14 out of 15 IoT data sets) of success rate for the soft computing based machine learning enhancement approach for privacy and security in macro layer IoT devices using cyber security techniques.

In near future this research will be extended for automated robotics based IoT devices privacy and security improvement using Artificial intelligence with robotics.

References:

[1] Tonge A. M., Kasture S. S., Chaudhari S. R., Cyber security: challenges for society-literature review, IOSR Journal of Computer Engineering (IOSR-JCE), e-ISSN: 2278-0661, p-ISSN: 2278-8727, 12(2), 67-75 (2013).

[2] Agarwal K., Dubey S. K., Network Security: Attacks and Defence, International Journal of Advance Foundation and Research in Science&Engineering (IJAFRSE), 1(3), 8-16 (2014).

[3] Homer J., Zhang S., Ou X., Schmidt D., Du Y., Rajagopalan S. R., and Singhal A.. Aggregating vulnerability metrics in enterprise networks using attack graphs, Journal of Computer Security, 21(4), 561–597 (2014).

[4] Cerrudo C., AnEmerging US (and World) Threat: CitiesWideOpen to Cyber Attacks; retrieved from https:// ioactive.com/pdfs/IOActive_HackingCitiesPaper_ CesarCerrudo.pdf, accessed on 30.09.2017.

[5] Kizza J. M., Guide to Complete Network Security, 4thEdition, Springer International Publishing, ISBN: 978- 3-319-55605-5 (2017).

[6] Noura, M., Atiquazzaman, M. and Gaedke, M. Interoperability in Internet of Things: Taxonomies and Open Challenges. Mobile Networks and Applications, 24, 796-809, (2020)

[7] IOT Analytics: Market Insight for IOT; Top 10 IoT Applications in 2020. https://iot-analytics.com/top-10-iot-applications-in-2020

[8] https://kaggle.com

[9] www.github.com

[10] https://www.kali.org/

[11] https://www.ossec.net/