International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 1
***Article Received:** 25 October 2022 **Revised:** 12 November 2022 **Accepted:** 30 December 2022*

Heuristic Machine Learning Enhancement Approach for Privacy and Security in Micro Layer IoT Devices Using Cyber Security Techniques

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

[1]Research Scholar
Department of Computer Science, St.Xavier's College, Tirunelveli - 627 002
Manonmaniam Sundaranar University, Tirunelveli – 627 012
Email: ebiroselin@gmail.com
[2]Associate Professor
Department of Computer Science
St Xavier’s College, Tirunelveli – 627 002
(Affiliated to Manonmaniam Sundaranar University, Abishekapatti, Tirunelveli – 627 012)

Abstract:

The current digital life is incorporated with IoT devices in which the communication from one entity to another entirely depends upon the electronic data signals with vast amount of information. The existing strategies to control these IoT devices are not in an easier state nowadays. Each IoT device handles its own type of data so that their communication system dependent data is always ready for their use and moreover it’s not feasible for them to provide security to their data. The distributed IoT device information system is a collection of data with different formats which requires more effort to handle it in an efficient manner by maintains the proper privacy and security. The process of identifying the IoT devices, cracking its communication strategy, understanding the security issues within the system is a complex process to implement. The existing methodologies focus on the IoT device features but resulted with improper classification and unrelated information data sets. This research article proposes a machine learning approach for identifying the micro layer IoT device privacy and security issues. In future this research paper will be extended with the implementation ofmachine learning based Macro level IoT devices privacy and security maintenance.

Keywords: Machine learning, IoT, Privacy data, Cyber security, Security

I. Introduction:

IoT:

Internet of things (IoT) describes devices with sensors, processing ability, software and other technologies that connect and exchange data with other devices and systems over the Internet or other communication networks.The term IoT, or Internet of Things, refers to the collective network of connected devices and the technology that facilitates communication between devices and the cloud, as well as between the devices themselves.

The incorporation of inexpensive computer chips and high bandwidth telecommunication, we now have billions of devices connected to the internet. This means everyday devices like toothbrushes, vacuums, cars, and machines can use sensors to collect data and respond intelligently to users.

Cyber Security:

Cyber security is the practice of protecting systems, networks, and programs from digital attacks. The term cyber-attacks are usually aimed at accessing, changing, or destroying sensitive information;

***Article Received:** 25 October 2022 **Revised:** 12 November 2022 **Accepted:** 30 December 2022*

extorting money from users through ransom ware; or interrupting normal business processes.

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 theheuristic machine learning enhancement approach for privacy and security in micro layer IoT devices using cyber security techniques. They are,

Stage-1: Machine learning based identificationof IoT device Type and its layer

a. Collect IoT device resources

b. Filter the communication

c. Find the IoT device type and layer through machine learning

d. List the Micro Layer IoT devices.

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

a. User's side view

b. Manufacturer's perspective view

c. Technical point of view

Stage-3: Machine learning approach to handle the issues

a.Supervised Learning

b. Semi Supervised Learning

c.Unsupervised Learning

d. Reinforcement Learning

Stage-4: Resolve privacy and security issues using cyber security techniques

a. Strong Password

b. Multifactor Authentication

c. Firewall

d. Software control

e. Backups

f. Security Manuel

Stage-5: Testing

Testing tools for privacy and security management

The proposed methodology of heuristic machine learning enhancement approach for privacy and security in micro layer IoT devices using cyber security techniques is as follows in Fig-1.

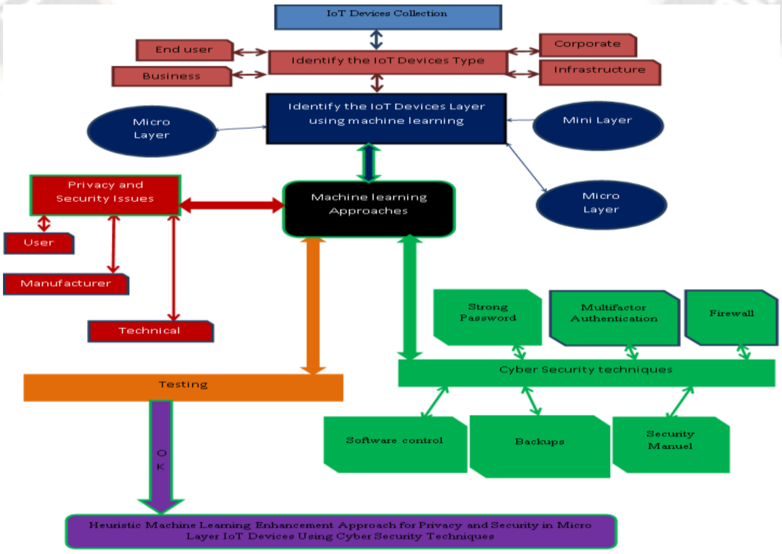
IoT Devices Collection
End user
Business
Identify the IoT Devices Type
Corporate
Infrastructure
Micro Layer
Identify the IoT Devices Layer using machine learning
Mini Layer
Micro Layer
Privacy and Security Issues
Machine learning Approaches
User
Manufacturer
Technical
Strong Password
Multifactor Authentication
Firewall
Testing
Cyber Security techniques
O K
Software control
Backups
Security Manuel
Heuristic Machine Learning Enhancement Approach for Privacy and Security in Micro Layer IoT Devices Using Cyber Security Techniques

Fig-1: Proposed heuristic approach for IoT privacy and security

Article Received: *25 October 2022* ***Revised:*** *12 November 2022* ***Accepted:*** *30 December 2022*

The algorithm for the heuristic machine learning enhancement approach for privacy and security in micro layer IoT devices using cyber security techniquesis as follows:

```
Start
Input: IoT devices collection with information
Step-1: Identify IoT device Type and its layer
        a. Collect IoT device resources
        b. Filter the communication
        c. Find the IoT device type and layer through machine learning
        d. List the Micro Layer IoT devices.
Step-2:Recognize the Issues related to privacy and security
        a. User's side view
        b. Manufacturer's perspective view
        c. Technical point of view
Step-3: Apply Machine learning approach to handle the issues
        a.Supervised Learning
        b. Semi Supervised Learning
        c. Unsupervised Learning
        d. Reinforcement Learning
Step-4:Resolve privacy and security issues using cyber security techniques
        a. Strong Password
        b. Multifactor Authentication
        c. Firewall
        d. Software control
        e. Backups
        f. Security Manuel
Step-5:  Testing
If all the above are success go to end
Else goto step-1
End if
End
```

III. Implementation

Stage-1: Machine learning based identification of IoT device Type and its layer

Stage-1 contains the following components for implementation:

a. Collect IoT device resources

The IoT devices are the collection of internet oriented communication devices.

i. Home appliances containing

- Lights
- Fan
- TV
- Speaker
- Fridge
- Washing Machine
- Dishwasher etc.,

ii. Activity trackers

- Smart watch
- Health Monitor
- Smart ring etc.,

iii. Industrial safety

- Fire Extinguisher
- Room Temperature
- Earth quake/Extreme Heat sensors etc.,

iv. Entertainment

- Augmented reality
- Virtual reality devices etc.

v. Tracking

- Vehicle
- Object
- Personnel etc.

b. Filter the communication

The communication are filtered as

- Audio alone

Article Received: *25 October 2022* ***Revised:*** *12 November 2022* ***Accepted:*** *30 December 2022*

- Visual display alone
- Motricity/Traction alone
- Combination of all.

c. Find the IoT device type and layer through machine learning

i.The IoT device types are classified as

- ✓ **End user devices**

IoT devices used by end users such as Google Home,Fire TV etc.

- ✓ **Business devices**

IoT devices are in practical use for business oriented purposes health monitoring, cloud storage.

- ✓ **Corporate Management devices**

IoT devices used for inventory management, supply chain management, safety etc.

- ✓ **Infrastructure devices**

IoT devices focus on smart city, waste management, and people safety.

ii. Machine learning based IoT device layer recognition

The machine learning based decision trees are used for recognizing the IoT device layers.

```
If the access of IoT device dominated by Human to Machine then
        IoT device Layer=Micro Layer
Else if the access of IoT device dominated by Machine to Human then
        IoT device Layer=Mini Layer
Else if the access of IoT device dominated by Machine to Machine then
        IoT device Layer=Mini Layer
Else
        IoT device Layer=Mixed*
End if
```

**-* represents the remaining communication Human to Human is a transitive relation such as Human~Machine~Machine~Human*

d. List the Micro Layer IoT devices.

- Biometric attendance
- Speech recognition
- Smart copier

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

It includes three dimensional view of affect as follows:

a. User's side view

- Inadequate Password Protection
  The common passwords used in IoT devices are "Adminadmin","12345678", "abcdefgh", easy to guess through administrator data etc. This leads to severe security issue and it will affects the privacy of users.
- Lack of Secure Interfaces
  The lack of Modem security configuration and device connectivity features impact the security in negative direction.
- Secret profiling
  The unknown collection of user information such as face, finger print, timings, and voice etc. mainly affects the privacy then with the security of the entire data collection.

b. Manufacturer's perspective view

- Limited Compliance from IoT Manufacturers
  Some IoT devices only work with 2.4 GHz and some other may with 5G alone. Only few IoT devices compliance is with all the network configurations.
- Device Update Management
  The drawback in proper updates with the corresponding monthly security patches will affect the IoT devices effective privacy and security management.

c. Technical point of view

- Interrupting Interface
  Some IoT devices communication channel frequency affects other IoT devices,and then there may be privacy data leak with unknown server possibility.
- Unauthorized access

***Article Received:** 25 October 2022 **Revised:** 12 November 2022 **Accepted:** 30 December 2022*

The unauthorized users access the data with stolen credentials or hacks is an important security issue.

- ❖ Duplicity
  The redundant data in IoT directs the consolidated report with lot of ambiguity. The creation/modification of privacy data is also possible.
- ❖ Malfunctioning
  The malfunctioning or wrong data entry affects the security of the entire entity which will affect the personnel's involved in the entire process.

Stage-3: Machine learning approach to handle the issues

a. Supervised Learning

Supervised learning approach plays the vital role in handling the user side view in privacy and security issues of password protection, secure interface and handling secret profiling.

The steps are as follows:

Step-1:Collect the prior knowledge about the customer and IoT devices.

Step-2: Apply supervised learning with prior knowledge of correct data format.

Step-3: Target device password, change with cyber security techniques.

Step-3: Focus Router configuration, apply essential cyber security encryption algorithms.

Step-4: Analyze local storage in IoT device; perform anomaly detection using cyber security for deletion.

Step-5: Continue steps 1to 4 until all the issues are solved.

b. Semi Supervised Learning

Semi Supervised learning approach plays the important role in handling the manufacturer perspective view in privacy and security issues of limited compliance and device update management.

Step-1: Apply semi supervised learning approach with accept or reject options.

Step-2: Set/purchase the router setup with 2 bands of Wi-Fi networks 2.4G and 5G which is known to the buyer.

Step-3: Connect the unknown IoT device with proper band using cyber security protocols.

Step-4: Reject the open Wi-Fi connection other than configured 2.4G/5G router.

Step-5: Check updates details then Accept/Reject based on the compliance nature of the IoT device.

Step-6: Continue steps 1to 5 until all the issues are solved.

c. Unsupervised Learning

Unsupervised learning approach is useful in handling the first partial Technical point of view in privacy and security issues such as interrupting interface and unauthorized access.

Step-1: Apply unsupervised learning approach with accept or delete modes.

Step-2: Find the unknown channel for IoT device in the router configuration.

Step-3: Fix the channel for the corresponding IoT using cyber security credential locks.

Step-4: If unwanted device connection found then delete else accept.

Step-5: Continue steps 1to 4 until all the issues are solved.

d. Reinforcement Learning

Reinforcement learning approach is useful in handling the second partial Technical point of view in privacy and security issues such as duplicity and malfunctioning.

Step-1: Apply reinforcement learning for trial and error mapping

Step-2: Collect the IoT local data storage information.

Step-3: Check for redundancy using XLStat tool if no duplicates continue else delete.

***Article Received:** 25 October 2022 **Revised:** 12 November 2022 **Accepted:** 30 December 2022*

Step-4: If error occurs learn it disconnect IoT device from network otherwise continue with cyber security.

Step-5: Continue steps 1to4 until all the issues are solved.

Stage-4: Resolve privacy and security issues using cyber security techniques

a. Strong Password

The complexity in password combination setting defines the security level to hack it with any algorithmic attacks; the more complexity password requires more amount of time to hack. The characters length starts from 8 to 15. The combinations are Capitals, small caps, digits, and special symbols.

The minimum desirable length =12 with a Max of 15

The following computation for password of length 12 combination defines the balanced complexity level

No of characters=12

1	2	3	4	5	6	7	8	9	10	11	12

No of components=4

The components are as follows:

{(A,B,C,,Z), (a,b,,z), (0,1,,,9), (@,#,$,%,,*)}

Balanced selection=3 characters from each component

E	B	Y	r	s	n	5	1	4	#	@	$

Non-concurrency occurrence=True

E	#	Y	r	@	s	5	B	4	n	1	$

Name/Birth/Anniversary year/car number etc. combination=False

Q	#	K	b	@	y	3	Z	6	x	8	$

The final password is stronger and balanced.

If the letter combinations are not extremes but with middle layer alphabets (to avoid trial and error from A/a-Z/z or Z/z-A/a) and rare character symbols are present in the combination

Then

The final string is the strongest and balanced one to crack.

b. Multifactor Authentication

The cyber security techniques suggests the following multi factor authentication for the IoT devices login procedures to connect to Modem or access the data from your network as in table-1.

Table-1: Multifactor authentication security level

Sl.No	Additional Factors	Security Level	Combination complexity to Crack
1	Password	20%	20%
2	OTP	20%	40%
3	Pin/Passkey	10%	50%
4	Finger Print	20%	70%
5	Face recognition	15%	85%
6	Retina/Voice	15%	100%
For any other combination the corresponding security levels are summed up.			

c. Firewall

The micro layer IoT device security is maintained by using the following two types of firewalls.

i.Web application firewall

Web application firewall controls the data transfer made from the IoT devices.

ii. State inspection firewall

State inspection firewall keeps track of the IoT devices which performs the abnormal communication.

d. Software control

The IoT device software are controlled through the following operations

i. Connect the IoT device for proper updating

ii. Ensure updated security patch

iii. Start and Stop the web communication.

e. Backups

The IoT devices are regularly connected to the local server to take the backups in a local device in order to ensure the data security.

f. Security Manuel

All the IoT devices must ensure the users with the proper understanding and knowledge about the smart product which are in use with the internet communication.

It includes the following:

i. Do's and Don'ts

ii. IoT device Net connectivity

iii. Communication and access

iv. Trouble shooting

v. Terminate the connection/Disconnect the device from Net.

Stage-5: Testing

The following testing tools are used for privacy and security management.

i. Tenable open source tool for testing [10] as in fig-2.

Tenable Nessus®

The first tool in your cybersecurity toolbox

Expose and close weaknesses across your constantly changing attack surface with the industry's most trusted vulnerability assessment solution.

Fig-2: Sample open source tool-1 for testing

ii. Rapid7metaspoiltopen source tool [11] as in fig-3.

metasploit

The world's most used penetration testing framework

Knowledge is power, especially when it's shared. A collaboration between the open source community and Rapid7, Metasploit helps security teams do more than just verify vulnerabilities, manage security assessments, and improve security awareness; it empowers and arms defenders to always stay one step (or two) ahead of the game.

Fig-3: Sample open source tool-2 for testing

IV. Results and Discussion

Consider the IoT device dataset from Kaggle standard data set [8] and Github [9] with a collection of 8 data resources along with the real time IoT device connection such as Face attendance IoT system, Finger print verification system data from different organizations.

Article Received: *25 October 2022* ***Revised:*** *12 November 2022* ***Accepted:*** *30 December 2022*

The proposed methodology gives the better privacy and security results by applying the proposedheuristic machine learning enhancement approach for privacy and security in micro layer IoT devices using cyber security techniques.

This research article gives 87.5% (7 out of 8IoT data sets) of success rate for the proposed heuristic machine learning enhancement approach for privacy and security in micro layer IoT devices using cyber security techniques.

The effective results between existing and proposed methods with the parameters such as precision, accuracy etc. are represented in the below Table-2 format,

Table-2: Proposed methodology parametric comparisons

No	Approach	Accuracy	Precision	Recall	F1 score value
1	Privacy and security management using existing cryptographic security approach using network security for connected devices.	53.6%	0.52	0.51	0.52
2	Heuristic machine learning enhancement approach for privacy and security in micro layer IoT devices using cyber security techniques	87.5%	0.87	0.89	0.88

The following fig-4 shows the performance comparison between the proposed and existing methodologies.

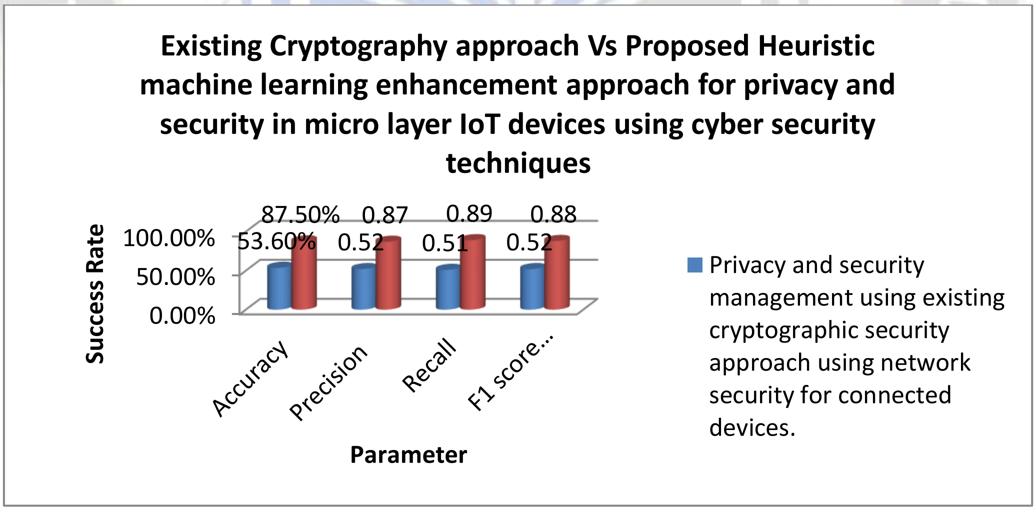

Fig-4:Proposed vs. existing methodology performance comparisons

V. Conclusion

Nowadays IoT devices are entering into our digital life in an exponential manner. The usage of internet access within home and external environment are also rapidly increasing. The IoT devices are certain type of entities connected in our day today life without knowing that sometimes it may act as a backdoor easy entry for attackers or hackers into our system to steal our privacy data and threatens the security of our entire network.

The researches in improving privacy and security in IoT device communication are all essential in our current life scenario. The proposed Heuristic machine learning enhancement approach for privacy

***Article Received:** 25 October 2022 **Revised:** 12 November 2022 **Accepted:** 30 December 2022*

and security in micro layer IoT devices using cyber security techniques initially focused with the IoT devices identification with its type, then focuses on IoT Layer recognition followed by the identification of micro layer IoT devices privacy and security issues, then focuses on the corresponding machine learning approach for solution identification followed by the proper Cyber security techniques for implementation and finally test the privacy and security efficiency.

This research article gives 87.5% (7 out of 8 IoT data sets) of success rate for the proposed heuristic machine learning enhancement approach for privacy and security in micro layer IoT devices using cyber security techniques.

In near future this research will be extended for Mini layer IoT devices privacy and security improvement using machine learning techniques.

References:

1. Tonge A. M., Kasture S. S., Chaudhari S. R., Cybersecurity: 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 enterprisenetworks 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.tenable.com/products/nessus
11. https://metasploit.com/