International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3
***Article Received:** 25 January 2023 **Revised:** 12 February 2023 **Accepted:** 30 March 2023*

Deterministic Machine Learning Enhancement Approach for Privacy and Security in Mini 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: drspvictor@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 IoT devices act as an essential component in our modern digital life for the effective day-today-life in our emerging communication system. The data communication among the IoT devices using the internet makes an open access possibility for affecting the privacy and security in a negative way for every device user's life. The process of handling privacy and security from machine to human communication is little bit complex when compared with human to machine communication. Each IoT device handles its own form of data so that their data communication system must be properly monitored with utmost care in order to provide security to their data. The existing methodologies focus on the IoT device connection and communication in the fast manner rather than with the focus on its privacy and security issues. This research article proposes a machine learning approach for handling mini layered IoT devices of machine to human communication devices privacy and security concern issues with its solutions. In future this research article targets with Macro layered IoT devices for the machine learning approach solution in privacy and security issues using cyber security techniques.

Keywords: Machine learning, cyber security, IoT, Data privacy, Security

I. Introduction:

Data privacy:

Data privacy is the relationship between the collection and dissemination of data, technology, and the public expectation of privacy, contextual information norms, and the legal and political issues surrounding them. It is also known as data privacy or data protection.

Data security:

Data security is the process of safeguarding digital information throughout its entire life cycle to protect it from corruption, theft, or unauthorized access. It covers everything such as hardware, software, storage devices, and user devices; access and administrative controls; and organizations' policies and procedures.

Cyber Security:

Cyber security refers to any technologies, practices, and policies for preventing cyber-attacks or mitigating their impact. Cyber security aims to protect computer systems, applications, devices, data, financial assets and people against ransom ware and other malware, phishing scams, data theft and other cyber threats. Cyber security is important because cyber-attacks and cybercrime have the power to disrupt damage or destroy businesses, communities and lives. Successful cyber-attacks lead to identity theft, personal and corporate extortion, loss of sensitive information and business-critical data, temporary business outages, lost business and lost customers and, in some cases, business closures.

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

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3
Article Received: *25 January 2023* ***Revised:*** *12 February 2023* ***Accepted:*** *30 March 2023*

computer programs that can automatically access data and perform tasks via predictions and detections.

II. Methodology

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

Stage-1: Filter the Mini layer IoT devices

a. Set Base layer=Micro layer
- Identify and filter the mini layer IoT device from the IoT resources.

b. List the Mini Layer IoT devices.
c. Understand the data.
d. Track the mechanism.

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

a. Lower level
b. Medium level
c. Higher level

Stage-3: Handle the issues using Machine learning techniques

a. Decision trees
b. Regression
c. Classification
d. Clustering
e. Association rules

Stage-4: Cyber security based privacy and security maintenance

a. Secure communication protocols
b. Software patches
c. Access control
d. Data integrity checks
e. Data flow control
f. Vulnerability assessment

Stage-5: Testing

Testing tools for mini IoT devices privacy and security management

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

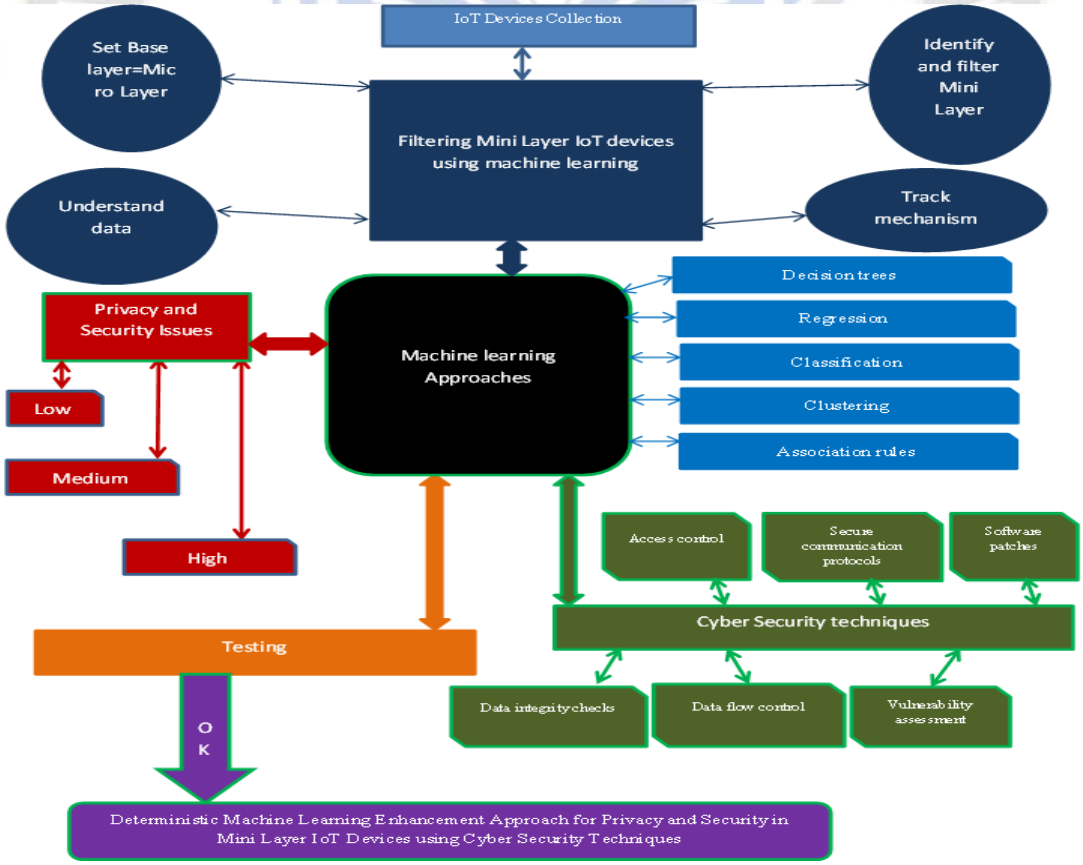

Fig-1: Proposed Deterministic approach for IoT privacy and security

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3
***Article Received:** 25 January 2023 **Revised:** 12 February 2023 **Accepted:** 30 March 2023*

The algorithm for the deterministic machine learning enhancement approach for privacy and security in mini layer IoT devices using cyber security techniques is as follows,

Start
Input: IoT devices collection with information
Step-1: Filter mini layer IoT device
a. Identify the mini layer IoT device from the IoT resources.
b. List the Mini Layer IoT devices.
c. Understand the data.
d. Track the mechanism.
Step-2: Identify the Issues related to privacy and security
a. Lower level
b. Medium level
c. Higher level
Step-3: Handle the issues using Machine learning techniques
a. Decision trees
b. Regression
c. Classification
d. Clustering
e. Association rules
Step-4: Cyber security based privacy and security maintenance
a. Secure communication protocols
b. Software patches
c. Access control
d. Data integrity checks
e. Data flow control
f. Vulnerability assessment
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 Mini layer IoT devices

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

Set Base layer=Micro layer

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

b. List the Mini Layer IoT devices.

i. Smart teapots.
ii. E-Alarm devices.
iii. IoT Traffic signal.
iv. E-Smoke detector.
v. Fitness monitor
vi. Fire alarms etc.

c. Understand the data.

IoT data formats are differentiated using machine learning based classification as in the following table-1.

Table-1: Machine learning based IoT data classification

Sl.No	Type	Format
1	Structured	Text
2	Semi structured	XML
3	Unstructured	Video/Audio streams

d. Track the working mechanism.

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

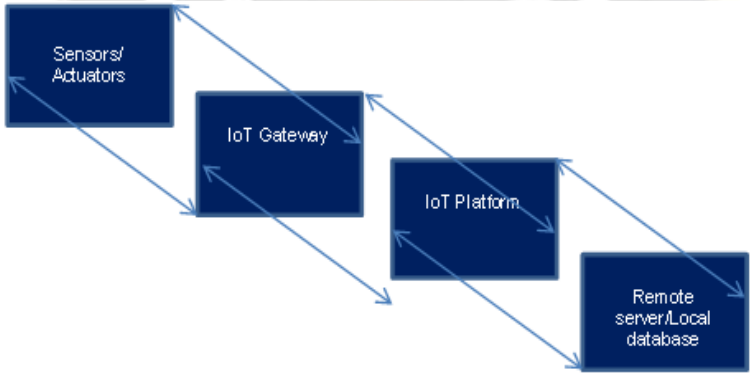

Fig-2: IoT working mechanism

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3
Article Received: *25 January 2023* ***Revised:*** *12 February 2023* ***Accepted:*** *30 March 2023*

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

a. Lower level

i. False alarm/Malfunction

The IoT deice produces wrong results highly deviated from the expected results due to certain errors caused by the system intentional or unintentional which lead to the security issue in an environment.

ii. Small scale attack

The process of attacking an IoT device through weak wireless connection and lead the connected devices to enter into the network of Botnets.

iii. Public exposure

Some IoT devices exposed the users Mail, mobile, profile photo whenever the product got registered in the network.

b. Medium level

i. Insecure data transfer

The data transfer from IoT devices are not encrypted so that the entire entity is in unsecured state during the working process or whenever the device got replaced or serviced. Data leaks and data corruption are the main medium level issues.

ii. Abundance of data

The vast amount of data created by the IoT devices is not handled properly so that the sensitive data are available in any IoT device at any time anywhere.

c. Higher level

i. Hackers IoT control

Hackers use the IoT devices to access and control the user's network devices, daily routines and setting up friends and foes.

ii. IoT Eaves dropping

An IoT device silently observes the data such as user's physical conversation, device conversation, viewable content information along with the user's presence in an entity or not data.

iii. IoT Ransom ware

Block the essential network devices and demands money for releasing the block with further normal functioning through IoT devices already present in the entity 9Home/organization).

Stage-3: Handle the issues using Machine learning techniques

a. Decision trees

Decision trees in Machine learning as in fig-3, fig-4 and fig-5 are used to deal with low level privacy and security issues.

i. False alarm/Malfunction

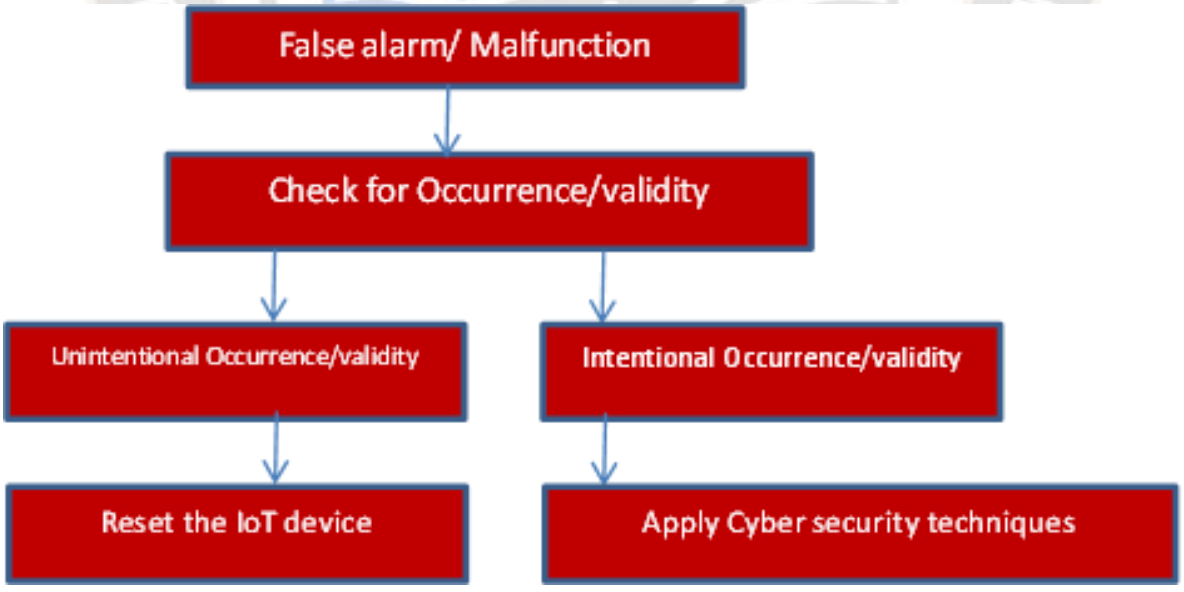

Fig-3: Machine learning decision tree based low level privacy and security issue handling-1

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3
Article Received: *25 January 2023* ***Revised:*** *12 February 2023* ***Accepted:*** *30 March 2023*

ii. Small scale attack

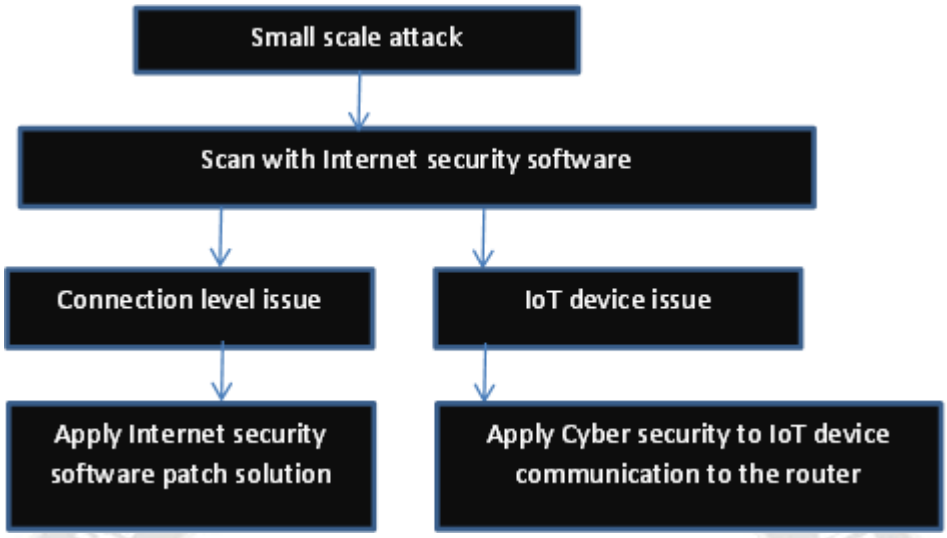

Fig-4: Machine learning decision tree based low level privacy and security issue handling-2

iii. Public exposure

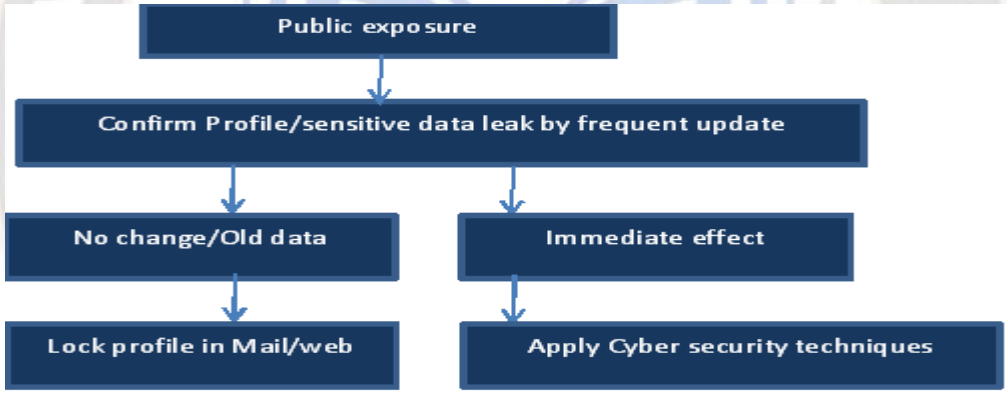

Fig-5: Machine learning decision tree based low level privacy and security issue handling-3

b. Regression

Regression in machine learning is used to deal the middle level privacy and security issues.

i. Data leaks and data corruption

The independent variables such as IoT connection ports, communication channel, transferred data that lead to data leaks and corruption such that it affects the dependent variable of effective data security.

Independent variables: IoT ports, channel, and data

Dependent variable: Secured data transfer

ii. Abundance of data

The vast amount of data storage affects the security in IoT devices with lot of independence in communication.

Independent variables: IoT devices, Local storage, servers

Dependent variable: Secured data storage

c. Classification

The machine learning based classification is used to handle high level privacy and security issue of IoT Eaves dropping.

If IoT net data usage=abnormal then

Eaves dropping level=1

Else if IoT response=low then

Eaves dropping level=2

Else if IoT state=off & Other IoT performance increases then

Eaves dropping level=3

Else if Idle time IoT data transfer=video/audio then

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3
***Article Received:** 25 January 2023 **Revised:** 12 February 2023 **Accepted:** 30 March 2023*

Eaves dropping level=4
Else if Idle time IoT device status = over heat/abnormal sound then
Eaves dropping level=5
Else
Check for other conditions
End if

d. Clustering

The clustering based machine learning approach is used to handle Hackers access control of IoT is as illustrated in table-2.

Table-2: Clustering based IoT security

Sl.No	Cluster name Access Control CluSter	Control based type	Attack area	Security measure
1	ACCS-1	Attributes	User policy rights	Revoke
2	ACCS-2	Discretionary	Owner rights	Reset
3	ACCS-3	Mandatory	Strict access	Cyber security approach
4	ACCS-4	Role	Hierarchy data	Cyber security approach
5	ACCS-5	Emergency	Essential data	Delete
6	ACCS-6	Rule	Time based data	Modify

e. Association rules

The association rules in machine learning is used to tackle the high level IoT ransom ware attacks

Rule-1: Attack level=suspect; Data=light corruption
Process: Restore the backup data and activate additional cyber security anti malwares

Rule-2: Attack level=light; Data=medium affected
Process: Apply commercial decryption process tools and activate cyber security additional anti malwares

Rule-3: Attack level=medium; Data=highly affected
Process: Apply system and network isolation and apply paid offline cyber security recovery software tools.

Rule-4: Attack level=High; Data=collapsed
Process: Report incident to clients and authorities to reduce further damage to them.

Stage-4: Cyber security based privacy and security maintenance

a. Secure communication protocols

The secure communication protocols play the vital role in handling low level privacy and security issues in mini layer IoT devices.

i. UpTLS

The upgraded secure socket layer with transport layer security protocol is used for high data transmission IoT devices.

ii. IETFCoAP

The Internet Engineering Task force identification of Constrained Application protocol is used for limited resource usage IoT devices.

b. Software patches

The following table-3 with the fuzzy membership value impacts the medium level privacy and security issue of mini layer IoT devices resolving capability. The more value resembles more security.

Table-3: Fuzzy membership table for software patch impact

Sl.No	Software Patch	Fuzzy membership value	Pointed Medium level issue
1	Missing data replacement	0.1	Insecure data transfer
2	Flash	0.2	Abundance of data
3	Recovery	0.3	Abundance of data
4	Firewall patch	1.0	Insecure data transfer
5	Security patch	0.9	Insecure data transfer
6	Service pack	0.8	Insecure data transfer
7	Hotfix	0.7	Insecure data transfer
8	Minor update	0.6	Abundance of data

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3
Article Received: *25 January 2023* ***Revised:*** *12 February 2023* ***Accepted:*** *30 March 2023*

9	Temp fix	0.4	Abundance of data
10	OS patch	0.5	Abundance of data

c. Access control

The ways to implement cyber security based access control to deal with high level privacy and security issue of hackers mini layer IoT control are,

- Mode-1: Defining the policies to the users to access the IoT with the internet.
- Mode-2: Enforce the rules/policies with strict monitoring.

There are four types of operations involved in cyber security based access control in IoT devices they are,

- Authorization: Credentials to login/connect the IoT device
- Authentication: Verify the credentials
- Identification: Identify the role
- Accounting: racking of logs

d. Data integrity checks

The data integrity check in cyber security is used for high level eaves dropping security issue in mini layer IoT devices. It includes the following processes.

Process-1: Check for data validity
Process-2: check for data error
Process-3: check for missing data
Process-4: check for abnormal data
Process-5: check for suspected /zipped encrypted data.

e. Data flow control

The data flow control is used to monitor high level security issue of eaves dropping. It verifies the following,

Step-1: Verify the connections
Step-2: Verify the transferred data
Step-3: Verify the download and upload data variations

f. Vulnerability assessment

The cyber security based vulnerability assessment prevents the high level issue of ransom ware in mini IoT devices. It includes the following steps:

Step-1: Perform Internet security based vulnerable test scan
Step-2: Assess the data and IoT interface application
Step-3: Give importance to the risks incidents with anti-malware tools.
Step-4: Continual and frequent vulnerability assessment.

Stage-5: Testing

Testing tools for mini IoT devices privacy and security management

The following testing tools as in fig-6 and fig-7 are used for mini IoT devices privacy and security improvement using cyber security techniques.

i. ZAP-Zed Attack Proxy-tool [10]

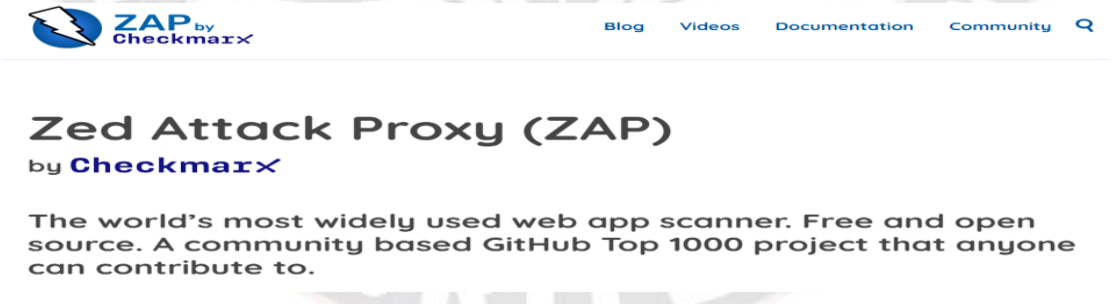

Fig-6: IoT privacy and security Testing tool-1

ii. Open VAS [11]

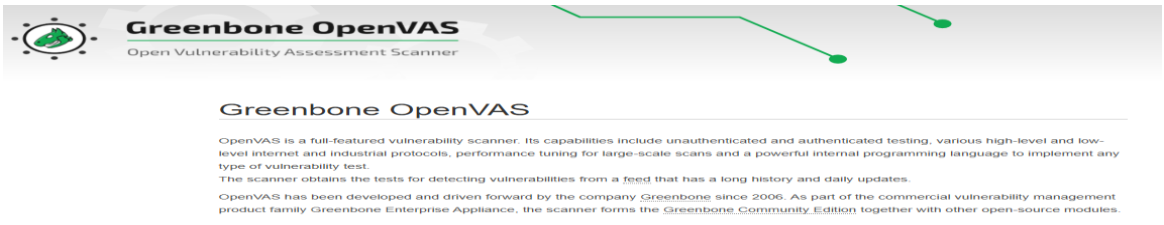

Fig-7: IoT privacy and security Testing tool-2

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3
Article Received: *25 January 2023* ***Revised:*** *12 February 2023* ***Accepted:*** *30 March 2023*

IV. Results and Discussion

The standard datasets from Kaggle standard data set [8] and Github [9] with a collection of 12 data resources along with the real time IoT device connection such as smart watch, smart TDS, E alarms from different brands.

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

This research article gives 91.7% (11 out of 12 IoT data sets) of success rate for the proposed deterministic machine learning enhancement approach for privacy and security in mini layer IoT devices using cyber security techniques

The effective comparison results between existing and proposed methods with the parameters such as recall, F1score etc. are represented in the below Table-4 format,

Table-4: Proposed methodology parametric comparisons

No	Approach	Accuracy	Precision	Recall	F1 score value
1	Privacy and security management using existing credential and non-credential vulnerability scan approach using cryptography for connected devices.	52.5%	0.51	0.50	0.51
2	Deterministic machine learning enhancement approach for privacy and security in mini layer IoT devices using cyber security techniques	91.7%	0.91	0.92	0.92

The following fig-8 shows the performance comparison between the proposed and existing methodologies.

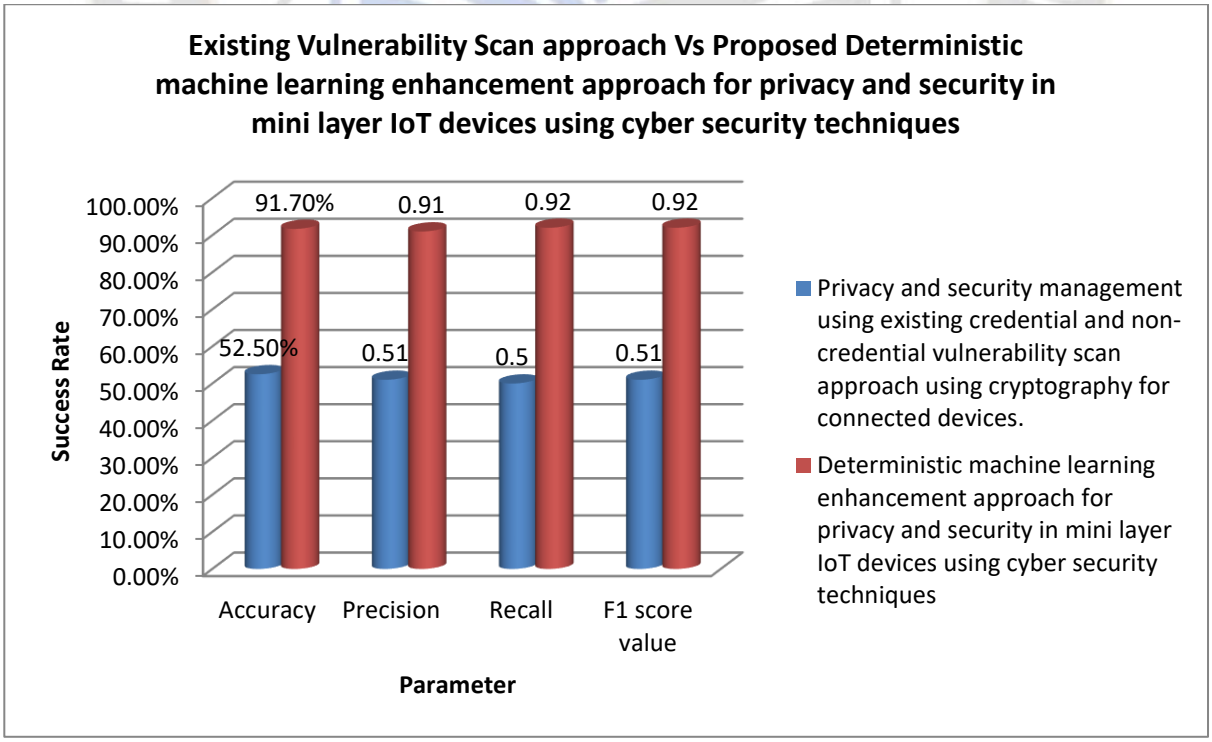

Fig-8: Proposed vs. existing methodology performance comparisons

V. Conclusion:

The dependency devices of human being are now added with the usage of IoT devices. The more amount of data transfer in IoT devices attracts the hackers or illegal users to misuse the IoT device of other for their selfish purpose or to damage the other person images.

The new researches in the field of IoT are essential to improve the privacy and security in IoT data transmissions along with the further tuning required for the development of safety environment in IoT device usage. The proposed deterministic machine learning enhancement approach for privacy and security in mini layer IoT devices using cyber security techniques initially focused with the IoT devices filtration with its mini type, then focuses on IoT data format recognition followed by the identification of mini layer IoT devices privacy and security issues, then focuses on the corresponding machine learning techniques for solution identification followed by the proper Cyber security techniques for implementation and finally test the privacy and security efficiency.

This research article gives 91.6% (11 out of 12 IoT data sets) of success rate for the deterministic machine learning enhancement approach for privacy and security in mini layer IoT devices using cyber security techniques.

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

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.zaproxy.org/
11. https://www.openvas.org/