ISSN: 2278-4632
Vol-12 Issue-12 No.02, December 2022

IOT APPLICATIONS SECURITY ISSUES AND SOLUTIONS – A STUDY

S.Jayalaxmi Assistant professor, Department of Computer Science, Bhavans Vivekananda College, Sainikpuri secunderabad 500056 : jayalaxmics79@gmail.com
S.Siddharth Student, Bachelor of Computer Applications(BCA) Bhavans Vivekananda College, Sainikpuri secunderabad 500056 : sidhu.sindhu39@gmail.com

Abstract. Internet of Things (IoT) has made human life easier as humans can remotely access all the interconnected devices by staying in a place. IoT is the system of unified devices, machines, and objects which are provided with a unique id. Everything and anything which is connected to a network come under IoT. The impact of global connectivity and the exchange of data created major significance on education, business, health care system, military capabilities, international trade, agriculture, and home applications. Cyber security is the major concern in this digital world to ensure protection from malicious activities, which aim to corrupt or steal data and interrupt an organization's systems with unauthorized access. Many new models and techniques are being proposed to protect the IoT network using Machine learning and Deep learning, Neural Networks, Block-Chain methods. In this survey paper, we reconnoitre on various IoT applications, its growth, specification, and the security challenge of layered structure. We analyse the presents challenges, issues that emerge in IoT network and provide a comparative analysis for the available solutions. We have also proposed a novel three-tier framework to control unauthorized access and identify suspicious internal activities in the private IoT network. This present survey is beneficial for industry and academia to categorize the challenges and issues in the current IoT security models and generate new dimensions of developments in it with advanced technologies.

INTRODUCTION TO IOT AND ITS EVOLUTION :

The past decades have perceived a rebellion in computing with related communications technologies. A portable digital system is the only solution for all day-to-day activities; the use of connected digital equipment has become an affluent tool for today's successful market. An easy and comfortable life is necessary for this fast-forward era, food to fashion, fast cash to fund transfer, a glossary to gadgets are accessible with one click. The solution for this is Internet of Things (IoT). IoT is system of interrelated computing devices, machines, objects, animals, or humans. Provided with unique identifiers and have ability to transfer data over network [1]. The number of connected devices in the network is rapidly growing as the population is increasing. currently the human population is about 7.9 billion and the number of connected devices is almost over 50 billion. At this rate the IoT industry will play major role in changing the graphs of some of the current industries. IoT will conquer the automobile and the enterprise industry [1]. Some of the automobile companies like Tesla has already started to integrate IoT with automobile in a very huge scale. We can see a very steep growth in the IoT in the coming years.

The reason for the same would be: -

- Decrease in the manufacturing cost of the sensors due to a huge demand.
- Decrease in the cost of data connections due to cloud storage solutions.
- Increase in the smartphone / tablet usage.

CONTRIBUTION

Our present survey focuses on various IoT applications and the threats with its effects. Main aim of the study to provide a view on available models, techniques, framework proposed using latest techniques. Our main contributionsare as follows.

- Highlighting security issues: We provide the list of attacks prone to each application of IoT and also discuss theeffects caused by each.
- Ephemeral View: Our study provides a brief overview of the most recent models and techniques proposed to secureIoT Home and Industry applications along with the challenges faced by other

ISSN: 2278-4632
Vol-12 Issue-12 No.02, December 2022

applications.

- Hybrid framework: We propose a hybrid framework to avoid the disadvantages raised by available techniques andapply the high-level security for each level.

ORGANIZATION OF THE PAPER

We organize the rest of the paper in the following sections. Section highlights the importance of security in IoTapplication with a focus on issues, attacks. Section discusses the vulnerabilities caused at each IoT layer. Sectionfocus on challenges faced by IoT industries, which include smart transport, agriculture, city and health. Section give a brief view on available techniques to establish a secured smart home application. Section Provide list of deep-learning based detection models which can be adapted for IIoT. Section propose a three level secured framework andfinally we end our study with Section conclusion and finding.

IOT SECURITY ISSUES AND CHALLENGES

With the increasing number of devices and sophistication of attack tools, a greater number of cyber threats, hacking, security breaches are getting reported. These are the appalling facts of network security and may create a catastrophe for the digital world if ignored. Many of the security measures have been proved ineffective because of burgeoning technologies like the public cloud, IoT, artificial intelligence, etc. Even now private networks are creating and facing data breach which can infiltrate sensitive data and damage digital channels [2]. These network attacks are categorized as social attacks that enter private networks as masquerade with spam mails and the network attacks which steal data directly by identifying weak network points or ineffective anti-virus services. Despite all the methods to improve and strengthen the protection mechanism, cyber criminals find out more and more sophisticated tactics to find out a loophole and tap into the connected devices, given them access to sensitive information [3]. Figure 1 provide list of security issues and challenges faced by IoT industry, and also emphasise some of the security controls and services provided to protect the data and environment.

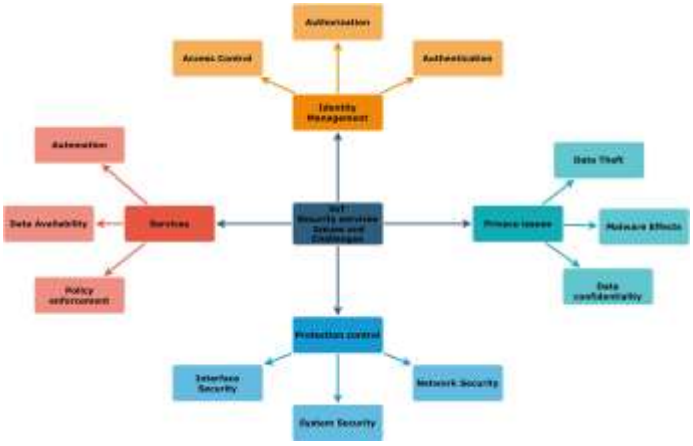

FIGURE 1. Security services, issues and challenges

Security service is an action to protect the network and data, identify various malicious activity and threats, these services are processed by selected security mechanism. A security mechanism is a protocol, method, or tool designed to implement a security service. Figure 1 represents various methods and techniques used to establish and maintain a secured connection, each service has a unique protection property. Confidentiality is a security service that safeguards data against unauthorized access or violating the privacy protocols this is implemented with data encryption. Data authorization is the process of specifying user id and password and data authentication is checking the credentials of the user. Integrity is the assurance that the message is unaltered, reminds the user with an alert message when violated. Data availability is a service that checks the protocols should not break data services, ensures 24*7 availability of data. More than one method is used for a selected service based on the complexity of the threat [3].

ISSN: 2278-4632
Vol-12 Issue-12 No.02, December 2022

LAYER WISE ATTACKS AND EFFECTS IOT

IoT structure follows dynamic architecture with an intelligent integrated infrastructure using interconnected heteroge- neous devices including sensors, gateways, device, and application platforms. However, it uses a primitive three-layer architecture. The first layer consists of physical and sensor devices; network and connectivity devices are placed in the middle layer; applications used for interactions are designed in the third layer. The three layers with security attack and effects are given in Figure2.

Apart from the traditional three layer architecture given in Figure2, an additional support layer is used for informa- tion exchange and to implement data control measures. Furthermore, some architectures also use a business layer to manage the complete IoT system as a business application [4]

The perception layer This is made up of physical and sensor devices. It recognizes the environment, collects relevant data, and sends it to the server. It is extremely sensitive and more vulnerable to attack. Some of the most common threats in this layer are node capture, eavesdropping, replay attacks, fake node inclusion, and timing attacks [5].

Network Layer: This layer is in charge of data transmission between smart things, network devices, and servers via wired or wireless medium. This serves as a connection point between the presentation and application layers.This layer is extremely sensitive, but particularly vulnerable to dangerous threats such as DoS and Man-in-the-Middle (MiTM) [5]. Furthermore, other network-related attacks appear to be negotiable.

Application Layer: It defines various applications that are used to control and monitor the connected devices. It serves as a bridge between the connected device and the user. This serves as a bridge between the end nodes and the network, allowing them to communicate with the authorised software components.

Support Layer: Three-level architecture is not very secure because information is passed directly to the network layer, allowing multiple threats to infiltrate. To address these flaws and protect against threats, a new support layer was proposed, resulting in a four-level architecture. The perception layer's data is authenticated using pre-shared secret keys and passwords before being transmitted to the network layer. DoS attacks, malicious insiders, and unauthorised access are examples of attacks that affect the support layer [6].

FIGURE 2. IoT Layers with Attacks and Effects

IOT APPLICATIONS ISSUES AND CHALLENGES :

This rapid growth of the IoT Industry will change the world we live in. e.g., there will be smart vehicles developed which will automatically send messages to the concerned person if we are late to the destination [1]. IoT will become industry specific, separate solutions will be designed for industries and there will be an increase in demand for specific usage. The next era to take the IT world to new heights is IoT, which transforms digital connectivity into integrated device connectivity. A revolutionized inter-communication between people, objects, data with a smart transformation and object communication is established by IoT. Information and communications technologies are used to make the critical infrastructure components and services for smart city conversion, smart education, healthcare, public safety, transportation, smart agriculture, and many interactive and efficient applications.

ISSN: 2278-4632
Vol-12 Issue-12 No.02, December 2022

IoT Applications

This section discuss about different industries which will adapt IoT and grow in the future. There are industries like healthcare and automobile which we can see are currently using IoT in their products, automobile company like Tesla has used IoT tools in its cars [2]. Some of the applications of IoT are discussed below:

- Smart health care used for tracking patient details, doctor availability, personnel tracking, real-time patienthealth status monitoring, Predictive expertise information for assistance.
- Smart marketing and controlling the commercial structure with retail and logistics supply chain control, Artifi- cial Intelligence(AI) based shopping applications, smart invoice management, item tracking, Fleet Tracking.
- Smart transportation through real-time tracking and information transferring methods for optimized path iden-tification , and generate shortest-travel time.
- Smart Home applications for energy conservation, device availability checking, surveillance camera, remotesensing for object control.
- Environmental Monitoring Air Pollution, Noise Monitoring, Waterways, Industry Monitoring.
- smart Agriculture: Smart Mapping, Smart crop monitoring, climate monitoring and forecast,live tracking, Geo-fencing, Green Houses, Compost, Irrigation Management, Soil Moisture Management.

Security issues and IoT attacks

However, there exist several challenges that affect the growth of the IoT. Lack of standardized techniques, heteroge- neous device connectivity, cost and memory expandable, etc. The research committee is providing many standardiza- tion techniques for IoT to strengthen the IT field. Digital accessibility is essentials in this current era, where security becomes a big challenge. Privacy protection, maintaining confidentiality, and integrity evaluation are maintained and managed using an automatic detection system. Multiple techniques have evolved in the past decades but, most of the models were limited to the result of research, lacking real-time implementation. Dangerous internal attackers can eas- ily bypass the traditional firewall security. IoT devices have spread widely and with greater development in all aspects of life in recent years, and with this advancement, new security challenges emerge. This paper focuses on the various IoT applications and emphasis security issues and solutions. Some of the common attacks for all IoT applications arediscussed below:

- Routing attacks: intermediate malicious nodes may modify the routing path and infect the system during thedata collection and forwarding process.
- DoS attacks: Due to the heterogeneity and complexity of IoT networks, network layer vulnerabilities exist. DoSattacks use three main methods: exhaustion, collision, and unfairness.
- Data transit attacks: Various attacks on data integrity and confidentiality occur in core networks during datatransit.
- Spoofed Routing Information: Attackers spoof, alter, or replay IP addresses to disrupt network traffic, resultingin routing loops, fake error messages, and shortened routes, among other things.
- Selective forwarding: A malicious or altered hub may change the IP address of the traffic by dropping somemessages and sending others, which are then debased.
- Man in the Middle attacks: When the attackers jam to gain access to the information. It primarily includes threetypes of attacks:
  - Eavesdropping: This is a passive attack in which the attacker gains access to the communication channeland modifies the received packets before sending them to all.
  - Directing assault: Assailants may alter the steering data and create a steering circle in order to fundamen-tally diminish the nature of administrations.
  - Attackers capture a signed packet and gain the trust of the destined entity by re-sending it to the sender later. It modifies the message sequence numbers and authentication code, as well as acting as the true sender.

ISSN: 2278-4632
Vol-12 Issue-12 No.02, December 2022

Other IoT applications and their issues

Cyber-attacks in digital infrastructure, are a typical increasing in twenty-first century. Reliance on digital communica- tions has made us vulnerable to attacks that might substantially disrupt global digital infrastructures, made possible by high-speed wireless data transmission technology. Financial markets, telecommunications, healthcare, transportation, national security, and other technology-driven industries are examples of such infrastructures. Therefore, cyber- terrorism and a large-scale cyber-attack could have catastrophic effects on our contemporary world. Figure 3 project various IoT applications with their applications and the security threat.

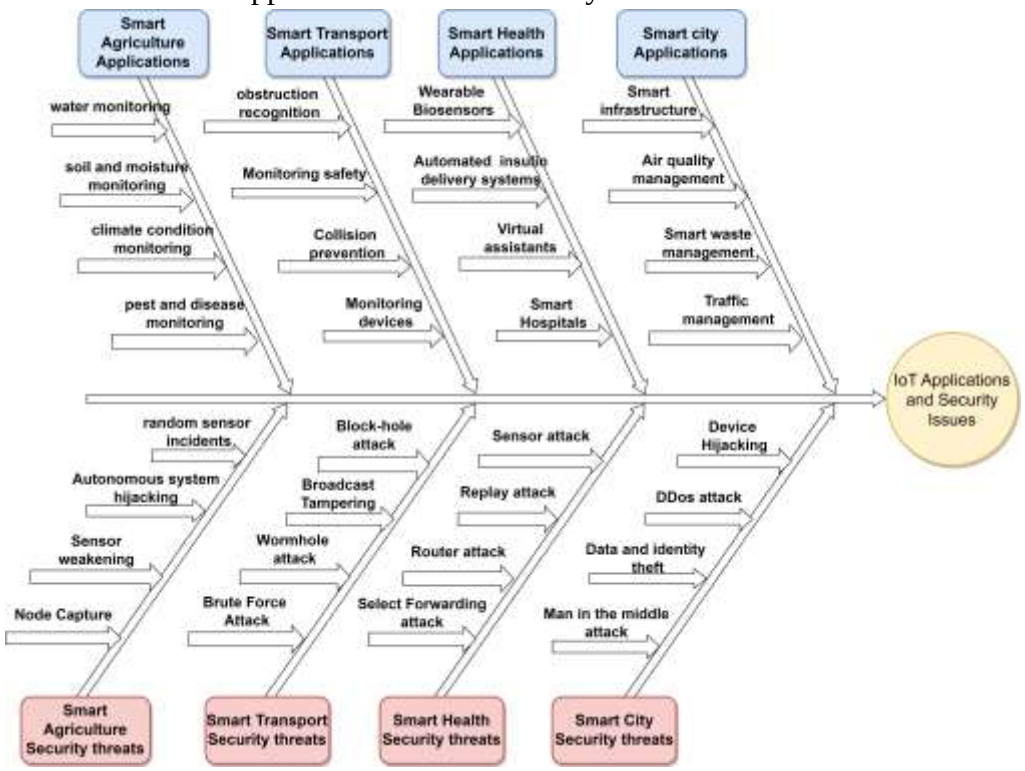

FIGURE 3. IoT applications and security threats

IoT Agriculture Risk and challenges: Similar to other industries, agriculture is being altered by digital tech- nology. In order to ensure that crops and soil receive the exact nutrients they require for optimum health, precision agriculture is becoming more and more popular. Drones, intelligent sensors, smartphone apps, and cloud computing are all essential components of precision agriculture. Organizations involved in food and agriculture are being targeted by ransomware hackers, which might interrupt operations. "As a result of ransom payments, lost productivity, and cleanup expenses." Along the process, they might also erode client confidence.

IoT Health Care risk and challenges: The flaws in healthcare IoT have been the focus of numerous public debates in recent years. The FDA has mandated that medical device manufacturers incorporate security into their systems as of 2016 and 2018. But the attacks are becoming more sophisticated: in 2017, the WannaCry ransomware impacted numerous healthcare facilities' operations by preventing staff from accessing crucial equipment. During the COVID- 19 outbreak in 2020, there was a subsequent spike in IoT attacks, with medical devices becoming the most popular targets of attackers.

General Solutions to secure the IoT Devices

- Closing the connection points when not used.
- Choose IoT devices that are easy to harden and update.
- Update and install recent firmware on IoT systems.
- Mon-IoT systems are patched in the operating system, firmware, security software, and web surfing tools.
- Configure the system for data encryption, remote wiping, creating unique passwords, two-factor authentication,backups, VPN connections, and virus elimination.

ISSN: 2278-4632
Vol-12 Issue-12 No.02, December 2022

- Enable two-factor authentication on all devices.

SMART HOME ISSUES AND SOLUTIONS :

An intruder can exploit security flaws and take control of the network. In addition to the security issues discussed above for each layer, this section provides an overview of the security challenges at each IoT application, as well as solutions to each problem and tools/techniques.

TABLE 1. Smart Home Security Issues and Solutions

References	Proposal	Tools and Technique
[7]	Integrated component and created IoT ecosystem	EOS Block-chain
[8]	Task automation for multimedia services	Reinforcement learning and Deep Learning
[9]	Facial recognition system to detect anomalies and make accident-free	HAAR-Cascade algorithm and Local Binary Pattern Histogram algorithm.
[10]	QToggle a smart home prototype with multiple functionality	Detection of motions and anomaly
[11]	Certificate less online/offline encryption to identify attacks	Hyper-elliptic Curve Cryptosystem
[12]	Password-based Key agreement protocols	Automated, security protocol validation tool

All the above techniques are used to secure the smart home tools, by storing data in secured cloud [7],automatic task assessment [8],authorization [9],encryption [11]and authentication [12].

SMART INDUSTRY ISSUES AND SOLUTIONS :

Industrial IoT (IIoT) is a connected network structure with sensors and physical manufacturing devices operated by Industrial Control System (ICS) [13]. ICS is the centralized unit with the combination of Supervisory Control And Data Acquisition (SCADA) to access the external activities, Distributed Control Systems (DCS) to manage the shared component services, Programmable Logic Controllers (PLC) to configure and manage the industrial infrastructure.

The sensors collect information from connected physical components; they are then shared with centralized source for operation and evaluation or analysis. At the same time, risk prediction is high in this conditions, where the leaking of important information may result in critical data loss and life threatening for the workers [14]. Moreover, the traditional insecure protocols like Mod-bus/TCP are creating a security glitch and causing authentication issues. Some of the security issues faced by popular smart industry are discussed in Table 2.

TABLE 2. Smart industrial attacks

Reference	Industry	Attack
[15]	Chemical and pharmaceutical production	Stuxnet virus attack in 2010 on hydro power stations and nuclear power net- works in Iran. Over 60% of personal computers and devices were targeted.
[16]	Plant and machinery	Stuxnet worm attack accessing PLC on Irans nuclear plant.
[17]	Water supply	The destruction of a water utility pump through a SCADA System in November 2011.
[18]	Telecommunications	Data theft by node capture and false messages as legitimate user and disrupt normal operations.
[19]	Electricity production and distribution	Abrupt change of power consumption , gaining unauthorized access and manip- ulate private information such as a collection of account and billing.
[20]	Power supply and transportation	Jamming attacks to degrade or disable energy supply.
[21]	Gas pipeline and distribution	Ukraine's power grid hack, stolen credentials and shut down 30 substations in March 2016 to access confidential information.

IIoTs are extended from IoTs where industrial applications run with IoT backbone. Machine learning and Deep learning models have high popularity in creating a intelligent detection system. All the detection models discussed below are developed with a strategy to reduce memory usage,

ISSN: 2278-4632
Vol-12 Issue-12 No.02, December 2022

improve the detection rate, reduce the false rate and trace new attacks.

CNN and DNN based model by Lane et al. [22] implemented for pre-trained networks. OuT of four networks experimented AlexNet and DeepEar resulted in low consumption of memory comparatively. LSTM an extended RNN technique being most prominent for classification, Das et al. [23] proposed LSTM based device identification model. An Integrated model using inverse document frequency for optimal feature selection and LSTM for Bot attack identification by Hadda Pajouh et al. [24] is suitable only for small datasets. Azmoodeh et al. [25] botnet and malware detection model for battlefield things via the device's OpCode using the deep eigenspace learning approach resultedin computational complexity.

A bidirectional LSTM-RNN embedded model by McDermott et al. [26] for identification and conversion of attack signature into the numerical format performed well, but suitable for limited patterns. A stacked AE fog-enabled IoT devices detection model by Mcdermott et al. [26] resulted in low accuracy and long-running time. A Sequential Su- pervised Deep learning-based Intrusion Detection with multi-scale residual temporal convolutional (MS-Res) module by Abdel-Basset et al. [27] proved accurate for CIC-IDS2017 and CIC-IDS2018 datasets.

PROPOSED FRAMEWORK

Building high-level security for edge devices in the connected world is the most difficult task. Considering a lot of security models and techniques, it is observed that the security component should be extended to multiple levels instead of single-level to detect and prevent the anomalies. To justify this a 3-level security system can be established which can filter the risk of threats and provide a suitable secured architecture. Assumption of security model is

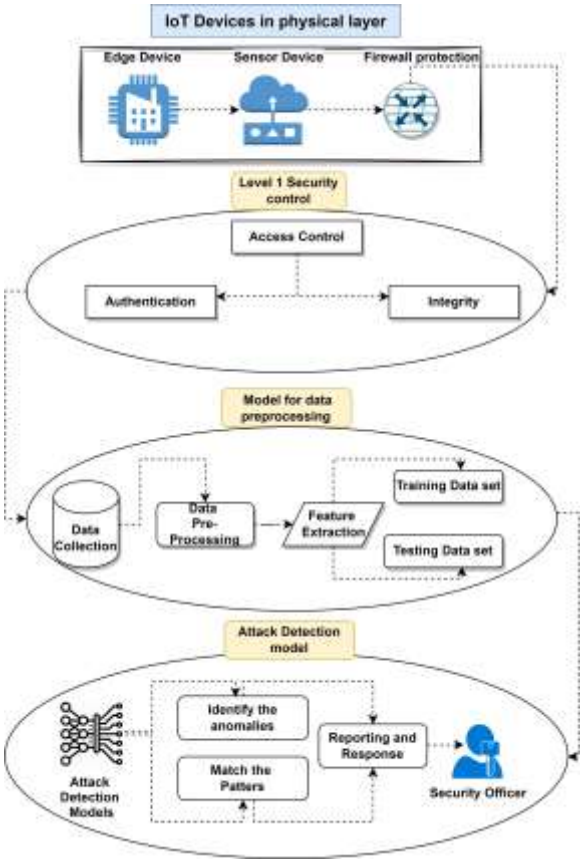

FIGURE 4. Proposed Framework

projected in Figure 4. The first level of security is formed with basic firewall protection, then the security services are applied to verify the authentication of the user, finally if any anomaly is observed the proposed detection model will identify and notify the alert message to the security officer.

ISSN: 2278-4632
Vol-12 Issue-12 No.02, December 2022

CONCLUSION

This survey focuses on various research works evolving around IoT security solutions for various applications. We have highlighted various threats and the issues caused by each layer. The study gave a light to some of the problem- solving techniques suitable for IoT home and industry. We have also provided a detailed summary on various attacks prone to smart health, agriculture, and smart city. This helps the reader to analyse the best solution for a selected problem. This survey analyses the results of the methods to provide a pathway to the new researchers in this domain. Finally, we have proposed a three-layer security model suitable for IoT network.

REFERENCES

1. A. Kamble and S. Bhutad, "Survey on internet of things (iot) security issues & solutions," in 2018 2nd International Conference on Inventive Systems and Control (ICISC) (IEEE, 2018) pp. 307–312.
2. S. Kiran and S. B. Sriramoju, "A study on the applications of iot," Indian Journal of Public Health Research & Development **9** (2018).
3. P. Jayalaxmi, R. Saha, G. Kumar, N. Kumar, and T.-H. Kim, "A taxonomy of security issues in industrial internet-of-things: scoping review for existing solutions, future implications, and research challenges," IEEE Access **9**, 25344–25359 (2021).
4. R. Seiger, U. Assmann, and S. Huber, "A case study for workflow-based automation in the internet of things," in 2018 IEEE International Conference on Software Architecture Companion (ICSA-C) (IEEE, 2018) pp. 11–18.
5. D. Singh, P. M. Mishra, A. Lamba, and S. Swagatika, "Security issues in different layers of iot and their possible mitigation," International Journal of Scientific & Technology Research **9**, 2762–2771 (2020).
6. M. Burhan, R. A. Rehman, B. Khan, and B.-S. Kim, "Iot elements, layered architectures and security issues: A comprehensive survey," Sensors **18**, 2796 (2018).
7. A. Tchagna Kouanou, C. Tchito Tchapga, M. Sone Ekonde, V. Monthe, B. A. Mezatio, J. Manga, G. R. Simo, and Y. Muhozam, "Securing data in an internet of things network using blockchain technology: smart home case," SN Computer Science **3**, 1–10 (2022).
8. A. Rego, P. L. G. Ramírez, J. M. Jimenez, and J. Lloret, "Artificial intelligent system for multimedia services in smart home environments," Cluster Computing **25**, 2085–2105 (2022).
9. V. Ravishankar, V. Vinod, T. Kumar, and K. Bhalla, "Sensor integration and facial recognition deployment in a smart home system," in Proceedings of the 2nd International Conference on Recent Trends in Machine Learning, IoT, Smart Cities and Applications (Springer, 2022) pp. 759–771.
10. C. Stolojescu-Crisan, C. Crisan, and B.-P. Butunoi, "Access control and surveillance in a smart home," High-Confidence Computing **2**, 100036 (2022).
11. S. Hussain, A. Alabrah, S. S. Ullah, H. Khattak, T. M. Alfakih, I. Ullah, et al., "An efficient online/offline signcryption scheme for internet of things in smart home," Wireless Communications and Mobile Computing **2022** (2022).
12. A. Huszti, S. Kovács, and N. Oláh, "Scalable, password-based and threshold authentication for smart homes," International Journal of Infor- mation Security , 1–17 (2022).
13. A. Hijazi, A. El Safadi, and J.-M. Flaus, "A deep learning approach for intrusion detection system in industry network." in BDCSIntell (2018) pp. 55–62.
14. C. A. Boye, P. Kearney, and M. Josephs, "Cyber-risks in the industrial internet of things (iiot): towards a method for continuous assessment," in International Conference on Information Security (Springer, 2018) pp. 502–519.
15. J. P. Farwell and R. Rohozinski, "Stuxnet and the future of cyber war," Survival **53**, 23–40 (2011).
16. N. Falliere, L. O. Murchu, and E. Chien, "W32. stuxnet dossier version 1.4," Symantec Security Response (2011).
17. A. A. Cárdenas, S. Amin, Z.-S. Lin, Y.-L. Huang, C.-Y. Huang, and S. Sastry, "Attacks against process control systems: risk assessment, detection, and response," in Proceedings of the 6th ACM symposium on information, computer and communications security (2011) pp. 355–366.
18. K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, et al., "Experimental security analysis of a modern automobile," in 2010 IEEE Symposium on Security and Privacy (IEEE, 2010) pp. 447–462.
19. F. G. Mármol, C. Sorge, O. Ugus, and G. M. Pérez, "Do not snoop my habits: preserving privacy in the smart grid," IEEE Communications Magazine **50**, 166–172 (2012).

ISSN: 2278-4632
Vol-12 Issue-12 No.02, December 2022

20. S. R. Chhetri, S. Faezi, N. Rashid, and M. A. Al Faruque, "Manufacturing supply chain and product lifecycle security in the era of industry 4.0," Journal of Hardware and Systems Security **2**, 51–68 (2018).
21. F. Tao, Q. Qi, A. Liu, and A. Kusiak, "Data-driven smart manufacturing," Journal of Manufacturing Systems **48**, 157–169 (2018).
22. N. D. Lane, S. Bhattacharya, P. Georgiev, C. Forlivesi, and F. Kawsar, "An early resource characterization of deep learning on wearables, smartphones and internet-of-things devices," in Proceedings of the 2015 international workshop on internet of things towards applications (2015) pp. 7–12.
23. R. Das, A. Gadre, S. Zhang, S. Kumar, and J. M. Moura, "A deep learning approach to iot authentication," in 2018 IEEE International Conference on Communications (ICC) (IEEE, 2018) pp. 1–6.
24. H. HaddadPajouh, A. Dehghantanha, R. Khayami, and K.-K. R. Choo, "A deep recurrent neural network based approach for internet of things malware threat hunting," Future Generation Computer Systems **85**, 88–96 (2018).
25. A. Azmoodeh, A. Dehghantanha, and K.-K. R. Choo, "Robust malware detection for internet of (battlefield) things devices using deep eigenspace learning," IEEE transactions on sustainable computing **4**, 88–95 (2018).
26. C. D. McDermott, F. Majdani, and A. V. Petrovski, "Botnet detection in the internet of things using deep learning approaches," in 2018 international joint conference on neural networks (IJCNN) (IEEE, 2018) pp. 1–8.
27. M. Abdel-Basset, H. Hawash, R. K. Chakrabortty, and M. J. Ryan, "Semi-supervised spatio-temporal deep learning for intrusions detection in iot networks," IEEE Internet of Things Journal (2021).