Vol. 3 No. 3 (2025)

Spectrum of Engineering Sciences

Online ISSN
3007-3138

Print ISSN
3007-312X

Exploring IoT Secuirty, Privacy and Data Protection

Muhammad Iqbal[1]
MS (CS) Scholar Bahria Univeristy, Islamabad. Iqbal_ktk19@ yahoo.com
M Arslan Sandila[2]
MS (IS) Bahria University, Islamabad. arslansandila@gmail.com
Zaheer Ul Hassan[3]
MS (CS) Bahria University, Karachi. zaheerulhassan@outlook.com

Abstract

Internet of things rapid growth is causing security and privacy concerns. Internet of medical things are devices designed for remote monitoring for the patients with chronic diseases. The security of the patient data at the collection, transmission and storage is critical for data integrity and privacy. The access to the patient data is limited only to users with high privileges i.e. for doctor and patient. On the other hand encrypted data is decrypted with shared keys by authorize user only. The technique is well suited for the access of data to only authentic users. The smart device connectivity with other devices is frequent that is sometimes raise questions related to security of these devices. The authentication of the devices is an important concern which is proposed this article. The authentication technique is robust as compared to other proposed technique due to having secure authentication at each step of devices to connect with main smart device. The Lightweight neural network method introduced for the network intrusion detection which is designed for IoT devices having low computing capability and low storage space. LNN model is excellent for classifying the smart devices traffic for normal and attack scenarios. In industrial IoTs trust management is the key factor to allow or deny the specific device to enter into the smart network. The trust between two nodes is calculated based on the device previous history with other devices. The approach is efficient for trust management based access to the devices. Fog assisted IoTs based on trust management and security component shows that their lightweight efficiency is higher as compared to other models for the security of resource constrained devices. For Industrial IoTs advanced encryption is best scenario where number of the devices frequently join and leave the

Spectrum of Engineering Sciences
Online ISSN
3007-3138
Print ISSN
3007-312X

network. The security measures at each level of the smart device is critical to security of data and privacy protection. The access based on human stored biodata or biometrics is secured enough for access to smart devices. The doubled encryption-decryption approach providing strong security measures for smart device generated data and users privacy. The Quick Response or QR code enabled technique providing critical information for device security enabled techniques increase buyer's trust, which is important for deployment of security enabled smart devices around the world.

Keywords: Internet of things security, data protection, privacy, data encryption, network intrusion detection, fog-assisted IoTs, Trust management.

Introduction

The internet of things are devices connected to the internet and also to each other includes smart home, smart lamps and smart cars etc. Increasing number of IoTs, welcoming security, privacy and data leakage issues. The manufacturers, cloud providers and researchers are working to mitigate these security issues in IoTs. As IoTs devices generate massive amount of data, the user's data protection an important concern to be resolved [1]. The unconscious use of IoTs devices, not changing default password, and lack of device updates lead towards the security of devices. These security problems enhance the data breach chances and make it easy for hackers to get control over the devices. Sometimes devices collect user data and share with third party without consent of user [2].

In IoTs security, authentication and authorization are important techniques to be followed. Authentication refers to who the user is and authorization refers to what permissions are given to IoTs user. Data encryption refers to encryption of plain text to cipher which is unreadable without the decryption keys. Secure Communication is another technique that ensures data transmitted between IoTs and other systems is secure from tampering. [3]. In terms of privacy, IoTs collect user personal data which also includes the sensitive data as well like financial statements. This data is shared with third parties without

Spectrum of Engineering Sciences
Online ISSN
3007-3138
Print ISSN
3007-312X
SPECTRUM OF ENGINEERING SCIENCES

knowledge of the user. The user should have control over the devices to limit the data collection to ensure privacy of the user data [4].

Due to high demand of Smart devices, the manufacturers only focus on bulk production of the device and compromising on the security of the devices. Later on, these devices are hacked by hackers are user data is leaked [5]. Each Device has different architecture and due to this it is not easy to make security applications for each device differently. This heterogeneity causes security problems as a result [6].

The current era focuses rapid increase in demand instead of taking security issues seriously in the field of Smart devices. The user focuses on bring your own devices without knowing the security problems [7]. General Data Protection Regulations are set of rules imposed by European Union, mainly focus on user data privacy [8].

Trustworthiness in IoTs ecosystem refers to performance of the devices with respect to security, privacy and data protection of the users [9]. The heterogeneity of IoTs architecture make it difficult to implement standard security protocols to overcome security issues. The standardization is

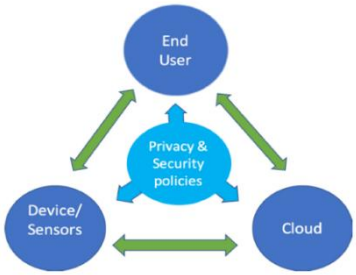

Figure 1. Internet of Things (IoT) Generic Model with Privacy and Security Policies.

an important to adopt to tackle security issues of the devices [10].

The figure above demonstrates the generic IoTs system, consist of End User, Cloud and Devices or Sensors. The device consist of sensors, those collect data and send to cloud for further processing of the data. The cloud of this system processes the data according to the needs of the users and performs accordingly. After the processed data is forwarded to end user. As it can be seen in the figure, among all these layers there is a privacy and security protocol ensuring the security of the data passing through layers IoTs system [2].

Spectrum of Engineering Sciences
Online ISSN
3007-3138
Print ISSN
3007-312X

Motivation

IoTs usage is rapidly increasing, creating smart life for the users as well welcoming many security issues is an hot topic now a days. The analysis of the security and data protection in this field an interesting experience to explore this research area and make some contributions in order to make improved and well organized measurements in order to mitigate risks in the security, privacy and protection of the date collected and shared by IoTs devices. Due to rapid adoption and emerging security concerns this field of research is a great experience to explore and work to make advancements in this field [4].

Research Contributions

The paper's contributions include:

- Its main impact is to recognize the IoTs security concerns arising due to flaws and vulnerabilities in device on network layers, application layer and edge layer.
- It's provides the security measures those should be implemented to avoid the misuse of the IoTs devices, the information generated by these devices.

The article is organized in the context that first covers overall introduction section giving overall overview of IoTs devices. In the next section, this paper shows an overview figure regarding security, privacy and data protection. Next section provides motivation behind this research. The last section includes research contributions in this field.

Literature Review

Ali Ghubaish et al. [11] explained that Internet of Medical things (IoMT) can be secured at three level of security i.e. securing data collection, securing data in transit and securing data in storage. Further the hierarchal access technique is used to patient data access to doctor and medical staff based on high and low privileged. In Securing data collection, the patient data is secured which is collected by sensors. Two-way factor authentication technique is used to protect patient data as one of the two factor is compromised the other provide security. The security protocols such as constrained application protocols (CoAP) are implemented for the data in transit. CoAP is specifically designed for the secure communication between the sensor and the gateways in the IoMT.

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

Security of data storage in cloud is essential. The cloud layer can be used to detect the suspicious activity through the logs of the connected devices. If there is any suspicious device trying the damage the patient data, can be detected. This way security of data storage is assured at the cloud layer of the IoMT.

Mourade Azrour et al. [12] discussed the enhanced authentication protocol for IoT which consists of adding new sensor node phase, user registration phase, login and authentication phase and password changing phase. In adding new sensor phase to existing sensor, the gateway generates random and particular Identity of Sensor as identifier and Secret shared between the gateway and the sensor. Before the deployment of the new sensor node, the information is stored into database for the future usage. The user registration phase consist of R1, R2 and R3 which are random numbers. In R1, user choose his identity combining user ID and any random number r1, password combination of user id, user password and random number r2 and then it is sent to gateway. In R2, the gateway computes V which is the combination of gateway private key, random number r3 and user password. Gateway stores V and sent back to the user. In R3, user stores V in the smart card. In login authentication phase there are five steps, in auth1 user entered information is sent to gateway with string a, and timestamp T1, the gateway in auth2 verifies the information and if it is valid it creates string b and timestamp T2 and sent to the sensor. The sensor in auth3, checks the received information and if it is valid it generates string c and timestamp T3 and sent back to the gateway. In auth4, gateway checks timestamp and valid information and then generates string d and timestamp T4 and sent to the user in auth5, the user checks timestamp and if valid session is started. In password change phase, sensor authenticate the user information, gateway generated information and allows user to change the password. By implementing the technique, enhanced authentication is achieved for the security of IoTs.

It was elaborated by Ruijie Zhao et al. [13] the detection based on Lightweight neural network. To keeping in view the low computing capability of IoTs, lightweight neural network model has low complexity and size. Through Principal Component Analysis the dimensionality

Spectrum of Engineering Sciences
Online ISSN
3007-3138
Print ISSN
3007-312X

reduction reduced to overcome the complexity of the model. The datasets used are UNSW-NB15 dataset and Bot IoT dataset. In UNSW-NB15, 175341 records are used for training and 82332 records for testing. In Bot IoT dataset, training dataset have 363562 records and testing dataset 243043 records. In the data processing, label numerization and one hat encoding is used for converting text into binary form to make dataset lightweight. The lightweight Neural Network (LNN) model has low model complexity and consume less computational power due to dimensionality reduction and have high accuracy as compared to other machine learning techniques. The model helps in network intrusion detection for the security of IoTs.

It was discussed by Ikram et al. [14] the lightweight trust management for the security of the Industrial Internet of things. The lightweight trust management work on four parameters i.e. compatibility, cooperatives, delivery ratio and recommendation. When a trustee requests for the services from the trustor, the compatibility of the trustee i.e. the trust that node builds and stay with other nodes without any dispute is checked. On the other hand trustee cooperativeness refers to the cooperation of the trustee node with other nodes in the network. The delivery ratio of the trustee evaluates the delivery of the sent and received content between two interconnecting devices. The recommendation parameter of the trustee refers to the trust based release of the services based on the neighboring nodes interaction with the trustee node. When the trustee enter the network its identification is checked first, and then parameters compatibility, cooperativeness, delivery ratio and recommendation (C2DR) is checked. The threshold values lies between 0 to 10, 0 to 5 for no trust and 5 to 10 for trust. If trustee gains the threshold value >5 it is allowed to be connected to resources and if fails it is denied. If the new node is connected it's ID, parameters and threshold is checked and trust certificate is generated and saved into the database to allow or deny the trustee in the future. In this way lightweight trust management approach is used allocating the resources or connecting the devices to IoTs only based of the trust factor. It was discussed in [15] that proposed Fog IoT framework works on the security of the IoTs and trust management. The system model contains

Spectrum of Engineering Sciences
Online ISSN
3007-3138
Print ISSN
3007-312X

three layers i.e. IoT layer, cloud layer and node layer. In threat model cloud entities are divided as honest, IoTs and fog nodes as semi honest and malicious nodes as dishonest to establish the security of IoTs. Besides checking the malicious nodes, the trust factor is also checked computed by the node Quality of the Service and communication of the node with other nodes. In this way if after checking the trust level of the node, access to the node is given based on the control management which manages what privileged the node has. In this way security of the IoTs is assured.

It was elaborated by Martin Serror et al. [16] that encryption of the data is more important for the secure communication between the smart devices and cloud. The lightweight encryption and authentication is required to reduce the time in the process of encryption. In this regard, it was suggested that encryption of the data must be done first in order to reduce the time and making the communication faster. Before communication to cloud for the data storage or data access, the advanced encryption method helped in reducing the communication time as well as secure communication.

Dr. Sahar A. El_Rahman et al. [17] explained IoT security, privacy and data protection can be achieved by implementing security measures such as encryption, firewall at design level of IoTs device. There are three layers in IoTs i.e. perception layers, network layers and application layer. The security measures at each layer helps a lot to secure smart device at maximum level. At Perception layers the security threat are different and needs the implementations of the security measures to tackle these problems. The hackers attack this layer directly and launch DDOS attacks and making services unavailable for the users. The next layers is the communication layers which is responsible for the communication. At this level there should be authorization to limited to device to connect to the network to avoid heterogeneity of the different devices as it requires more resources to overcome security issues with different types of devices due to different architecture. The Application layers is the most important layer where the access to the device permitted only to authorized users others there are possibilities of the privacy and data leakage at this level.

Spectrum of Engineering Sciences
Online ISSN
3007-3138
Print ISSN
3007-312X

It was discussed in [18] that biometrics are used in IoT infrastructure for the authentication purposes. The authorized users are verified by IoTs devices based on their bio data such face, voice, handwritten signature and fingerprints. The person bio data is store already in order to give access to the user in the future. According the researcher, this method of biometrics more secure as the bio data pattern of the person is biologically different. The smart device after the verification of the person by checking bio data such as fingerprints, handwritten signature gives access to the user. In this way the unauthorized user involvement or access to the devices become very difficult to gain access to the smart devices and misusing the smart devices for the security aspects like leakage of the data, or getting unauthorized control over the smart device or tampering privacy of the users.

It was discussed in [19] that when IoT device like sensors collect data, the plain text is encrypted with the user private key and converted to first cipher text. At the next level it is again encrypted with DES or Data encryption standard algorithm and converted to the second cipher text. The IoT data generally comes in cloud where it is stored, processed and different algorithms are applied. When the second cipher text data come in cloud it decrypted by the DES algorithm. This data is now converted to first cipher text which was encrypted with the user private key. At the end when the data is finally comes at the destination it is decrypted with the user private key and converted to plain text or the data. The proposed approach ensures the data confidentiality, availability, authentication and authorization of the data.

It was elaborated by Dr. Hosein F. Badran et al. [20] that the people are more concerned about their privacy and protection of their personal data. As the IoTs devices security issues leads towards data leakage the people trust on the devices which are certified by different Government testing laboratories. The Approved Certification label on the devices make people to trust on the brand before purchasing the device. The different countries around the world like Australia, Canada, UK etc. has started implementing the rules to approve the IoT devices security test before launching into the market. The security certificate label on the devices with QR code help the user to know about the strong security

Spectrum of Engineering Sciences
Online ISSN
3007-3138
Print ISSN
3007-312X

measures implemented in the devices before getting smart devices.

Discussion and Evaluation

In Internet of Medical Things proposed approach by Ali Ghubaish et al. [11] provide security at three level i.e. at data collection, data in transit and data storage. The technique proposed for the securing data at the collection level is Two authentication approach which enables the security of the data in two first by encryption and then by biometrics. The advantages of the approach are it provides confidentiality, integrity and authentication and authorization for the usage of the IoT device. In Two way authentication if second factor is lost or hacked will result into data leakage and damaging security of IoTs. Securing data in transit approach has constrained application protocol for the secure transmission of data between the sensor and the gateway ensuring the secure transmission of data. If this protocol is compromised the data leakage happens. The data storage at the cloud level faces DoS attacks which makes the system unavailable for the users. The technique provides security of IoMT data at higher extent.

The proposed technique in [12] is robust enough to giving high security to access the IoT device by authenticated users only. From new sensor addition to password changing phase it is secure at higher extent preventing the password guessing attack, denial of service attack and insider attack. The Scyther Tool performance analysis shows that it has 13T computational cost which is less than other proposed techniques for the same scenario. The disadvantage is if user lost the information stored smart card resulting losing access to device.

Due to the resource constrained nature of IoTs devices [13], lightweight intrusion detection has advantage of working with these device as it has low complexity and size. The lightweight model neural network model size 54.86% and 61.69% less in size in Bot IoT and UNSW-NB15 dataset respectively. On the other hand the intrusion detection accuracy of LNN Model is 98.94% which 10% higher as compared to other models for the intrusion detection. The limitation of model is its data dependency.

The lightweight trust management approach [14] based on trust level threshold >5 giving access to node to connect or release the resources

Spectrum of Engineering Sciences
Online ISSN
3007-3138
Print ISSN
3007-312X
SPECTRUM OF ENGINEERING SCIENCES

for the requesting node. In this approach experimental results shows that where 800 nodes are connected to it, the delivery ratio remains stable i.e >0.5 out 1, showing the delivery ratio of trustee node is satisfied. On the other hand. The latency of trustee node becomes lower with time. The degree of trust for the trustee node remains >5 for the specific time to judge the device or the trust agent that node is trustworthy or not. If threshold value drops in specific time period i.e. <5, the node is rejected to access the device or claim the resource. Failure in detection of false node with fake trust level value resulting in access to malicious device.

The trust management in fog assisted IoTs [15] is remarkably ensured through the trust management component which provides access to connect with those device having the higher or specified trust value. This technique allows devices already having required trust level (>5) to directly connect to IoT. The trust management trained on 73 360 900 rows of dataset having 47 features, 80% data is used for training and 20% for the testing purpose which gives 98% accuracy for this data set. The disadvantage of this approach is that it totally depends upon the data for the training, if there is any discrepancy in dataset, the result will be false and hence the access will be given to lower trust value or infected device to connect with IoT device.

In Industrial Internet of things [16] multiple devices join and leave the network in the short time. The authentication of these devices for connected to the network is time taking as number of device is large and generate large amount of data as well. The proposed approach helps in encryption of data prior offloading it cloud and decrypted only the retrieved data at a time. This saves the computational cost by 30%. The disadvantage of this approach is that it does not work well where the data confidentiality is first priority.

The security of IoTs devices [17] at each layer i.e. perception, communication and cloud layer at the manufacturing level helps in mitigating the attacks on these devices. On the other hand the perception or sensor security helps in preventing DDOS attacks by hackers. The security of the communication layers mitigate the risk of unsecure data transmission between the sensor and the cloud layer. The cloud layer security enables the secure data storage. The failure to

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

achieve the security implementation, result into the data leakage and security and privacy of IoTs.

Due to different biological structure [18] of each person, the proposed approach has an advantage by storing the bio data such as face, voice, handwritten signature and fingerprints to give access to the users for the specific smart device. The disadvantage of this approach is that change in the bio data for the same person, does not allow him to connect to the smart devices. The process is again started for the verification of the person for the access which is time taking.

The encryption of data at two level [19] first when generated by device and then before storing into the cloud helps in achieving the security of the data. Then decryption process repeats the double decryption of the data to convert it to the plain text for user. The drawback of this approach is if the user private key is exposed the data decryption will be done plain text for user. The drawback of this approach is if the user private key is exposed the data decryption will be done by the hacker and data leakage will happen and thus damaging the security of IoTs data.

The proposed approach for QR code [20] for the consumer to know the implemented security approaches for smart device result into the selling of the device with strong security protocols. The advantage of the security label is that it contains the certifying authority sign, product and live QR code for scanning to read the product security measures. The limitation in this regard is the approach is not widely adopted and the manufacturing companies focus only on smart device production.

Conclusion and Future Work

Due to high demand of smart devices to make lifestyle convenient, the security of these devices has become extremely important. The main objective is to build a model for the IoTs security, privacy and data protection. In this article, an overview of smart devices security requirements at each level of architecture and security techniques were discussed. The other robust security techniques like hierarchical access, encryption of data, enhanced authentication, lightweight neural network for network intrusion detection, lightweight trust management, trust management with security component implementation, advanced

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

encryption, security implementation at device manufacturing stage, access based on biometrics, double encryption-decryption and QR code were discussed for the different scenarios for the security, privacy and data protection generated by smart devices. The each discussed technique was excellent for the security of the smart device based on the results compared by other techniques. The resource constrained nature (computing, power, storage) of IoT devices is the main difficulty in implementing the highly efficient security model for the security of these devices. The resource constrained nature of IoTs device needs to be addressed in the next study in future in order to deployment of the robust secure model. The future work also includes the implementation and deployment of these techniques in real world experiments in IoT devices for analyzing the performance in different scenarios with an objective to install cost-effective and highly efficient secure systems.

References

[1] Wei Zhou , Yan Jia, Anni Peng, Yuqing Zhang, and Peng Liu, "The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved", IEEE INTERNET OF THINGS JOURNAL, VOL. 6, NO. 2, APRIL 2021.

[2] Lo'ai Tawalbeh, Fadi Muheidat, Mais Tawalbeh, Muhannad Quwaider "IoT Privacy and Security: Challenges and Solutions", ACM, Applied Sciences 2022.

[3] Ghanshyam G. Parrkhede, Akshay Dilip Lahe, Bhushan L. Rathi, "A Study on Security and Privacy Challenges in the Internet of Things", IEEE, International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 2023.

[4] Abhijit SudamPavashe, Ankita Bajirao Sawant, Kishor Laxman Ghadage, "The Effect of Security and Privacy on the Internet of Things (IoT)", ReasearchGate International Journal of Advanced Research in Science Communication and Technology. 2021.

[5] Pradeep Jha, Riddhima Baranwal, Monika, Naveen Kumar Tiwari, "Protection of User's Data in IoT", IEEE Proceedings of the Second International Conference on Artificial Intelligence and Smart Energy, 2022.

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

[6] Kamran Shaukat, Talha Mahboob Alam, Ibrahim A. Hameed, Wasim Ahmed Khan, Nadir Abbas, Suhuai Luo, "A Review on Security Challenges in Internet of Things (IoT)", IEEE Proceedings of the 26th International Conference on Automation & Computing, 2021.

[7] Chalee Vorakulpipat, Ekkachan Rattanalerdnusorn, Phithak Thaenkaew, Hoang Dang Hai, "Recent Challenges, Trends, and Concerns Related to IoT Security: An Evolutionary Study", IEEE International Conference on Advanced Communications Technology, 2022.

[8] Malti Bansal, Marshal Nanda, Md. Nazir Husain, "Security and privacy Aspects for Internet of Things (IoT)", IEEE Proceedings of the Sixth International Conference on Inventive Computation Technologies, 2021.

[9] Nader S. Labib, Matthias R. Brust, Gregoire Danoy, Pascal Bouvry, "Trustworthiness in IoT – A Standards Gap Analysis on Security, Data Protection and Privacy", 2021 IEEE Conference on Standards for Communications and Networking.

[10] Jibran Saleem, Mohammad Hammoudeh, Umar Raza, Bamidele Adebisi, Ruth Ande, "IoT Standardisation - Challenges, Perspectives and Solution", ACM, Proceedings of the 2nd International Conference on Future Networks and Distributed Systems, 2021.

[11] Ali Ghubaish, Tara Salman, Maede Zolanvari, Abdulla Al-Ali, Raj Jain, "Recent Advances in the Internet-of-Medical-Things (IoMT) Systems Security", IEEE INTERNET OF THINGS JOURNAL 2021.

[12] Mourade Azrour, Jamal Mabrouki, Azedine Guezzaz, Yousef Farhaoui, "New Enhanced Authentication Protocol for Internet of Things", IEEE BIG DATA MINING AND ANALYTICS JOURNAL 2021.

[13] Ruijie Zhao, Guan Gui, Zhi Xue, Jie Yin, Tomoaki Ohtsuki, Bamidele Adebisi, Haris Gacanin, "A Novel Intrusion Detection Method Based on Lightweight Neural Network for Internet of Things", IEEE INTERNET OF THINGS JOURNAL 2022.

[14] Ikram Ud Din, Kamran Ahmad Awan, Ahmad Almogren, Ayman Altameem, Mohsen Guizani, "LightTrust: Lightweight Trust Management for Edge Devices in Industrial Internet of Things", IEEE INTERNET OF THINGS JOURNAL 2023.

Spectrum of Engineering Sciences
Online ISSN
3007-3138
Print ISSN
3007-312X

[15] Aisha Kanwal Junejo, Nikos Komninos, Julie A. McCann, "A Secure Integrated Framework for Fog-Assisted Internet-of-Things Systems", IEEE INTERNET OF THINGS JOURNAL 2021.

[16] Martin Serror , Sacha Hack , Martin Henze , Marko Schuba, Klaus Wehrle, "Challenges and Opportunities in Securing the Industrial Internet of Things",IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, 2021

[17] Dr. Kahkashan Tabassum, Dr Ahmed Ibrahim, Dr Sahar A. El_Rahman, "Security Issues and Challenges in IoT", 2021 IEEE CONFERENCE ON IoT SECURITY.

[18] Fadi Al-Turjman, Hadi Zahmatkesh, Ramiz Shahroze, "An overview of security and privacy in smart cities' IoT communications", 2021 WILEY SPECIAL ARTICLE ON IoT.

[19] Nishat tasnim Newaz, Mohammad Rafiqul Haque, Tajim Md. Niamat Ullah Akhund, "IoT Security Perspectives and Probable Solution", IEEE, 2021 Fifth World Conference on Smart Trends in Systems Security and Sustainability.

[20] Dr. Hosein F. Badran, "IoT Security and Consumer Trust", ACM, (2021) Proceedings of the 20th Annual International Conference on Digital Government Research