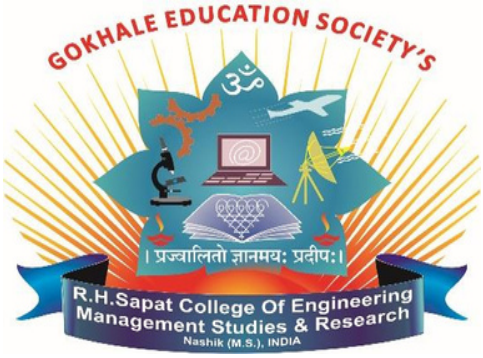


Savitribai Phule Pune University
Gokhale Education Society's

R. H. Sapat College of Engineering, Management Studies and Research,

Nashik - 422 005, (M.S.), INDIA

DEPARTMENT OF COMPUTER ENGINEERING

Third Year Computer Engineering

Year 2023-2024

Roll No: 08

Name of Student: Bhandari Ayushi Manish

Mobile No.: (+91) 8483815019

e- Mail ID: ayushibhandari28@gmail.com

Seminar Title: Emerging threats in loT Security

Seminar Guide: Dr.N.A.Deshpande

Area of the Seminar: Cyber Security

Abstract

The Internet of Things (IoT) marks the dawn of a new era of communication. By leveraging IoT technology, physical objects can transmit, receive, and exchange data in a seamless manner. Numerous IoT applications aim to automate a range of tasks and empower non-living objects to operate independently. These applications hold immense potential to enhance comfort, efficiency, and automation for users. However, realizing this vision requires a focus on security, privacy, authentication, and attack recovery to ensure a robust IoT infrastructure.

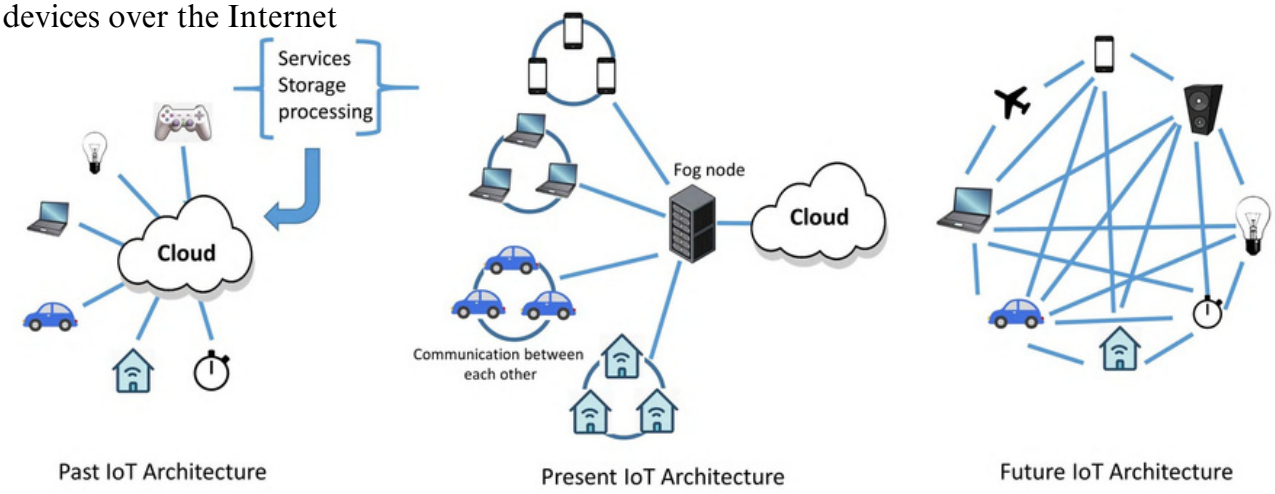
To achieve end-to-end security in IoT environments, architectural changes must be implemented. This paper provides a detailed review of the security-related challenges faced by IoT applications and the sources of threat. Additionally, the paper examines various emerging and existing technologies that enhance trust in IoT applications.

Specifically, the paper delves into four technologies, including blockchain, fog computing, edge computing, and machine learning, that can significantly improve the security of IoT.

Briefs about contents:

Introduction:

The pace of connecting physical devices around us to the Internet is increasing rapidly. According to a recent Gartnerreport, there will be around 8.4 billion connected things worldwide in 2020. This number is expected to grow to 20.4 billion by 2022 [1]. The use of IoT applications is increasing in all parts of the world. The major driving countries in this include western Europe, North America, and China [1]. The number of machine to machine (M2M) connections is expected to grow from 5.6 billion in 2016 to 27 billion in 2024.This leap in numbers itself declares IoT to be one of the major upcoming markets that could form a cornerstone of the expanding digital economy. The IoT industry is expected to grow in terms of revenue from $892 billion in 2018 to $4 trillion by 2025. M2M con-nections cover a broad range of applications like smart cities,The associate editor coordinating the review of this manuscript and approving it for publication was Alberto Cano. smart environment, smart grids, smart retail, smart farming, etc.Figure 1 shows the past, present and future architecture of IoT. In future, the devices are not only expected to be connected to the Internet and other local devices but are also expected to communicate with other devices on the Internet directly. Apart from the devices or things being connected, the concept of social IoT (SIoT) is also emerging. SIoT will enable different social networking users to be con-nected to the devices and users can share the devices over the Internet



With all this vast spectrum of IoT applications comes the issue of security and privacy. Without a trusted and interoperable IoT ecosystem, emerging IoT applications cannot reach high demand and may lose all their potential. Along with the security issues faced generally by the Internet, cellular networks, and WSNs, IoT also has its special security challenges such as privacy issues, authentication issues, management issues, information storage and so on.

a detailed survey of IoT security solutions in the existing literature is presented. First of all, the fundamental constraints to achieve high levels for security in IoTapplications are presented. The goal of this paper is to highlight the major existing and upcoming solutions for IoTsecurity. Specifically, the four major classes of IoT securitysolutions namely: (1) blockchain based solutions; (2) fog computing based solutions; (3) machine learning based solu-tions and (4) edge computing based solutions are highlighted.

Methods

- ## IoT SECURITY USING BLOCKCHAIN

Blockchain and IoT are important technologies that will have a high impact on the IT and communication industry.These two technologies focus on improving the overall transparency, visibility, level of comfort and level of trust for theusers. The IoT devices provide real-time data from sensors and blockchain provides the key for data security using a distributed, decentralized and shared ledger

The basic idea behind the blockchain is simple: it is adistributed ledger (also called replicated log files). The entries in the blockchain are chronological and time-stamped. Each entry in the ledger is tightly coupled with the previous entry using cryptographic hash keys. A Merkle tree is used to store the individual transactions and the root hash of the tree is stored in the blockchain. In the figure, T 1, T 2, T 3, · · · , Tn represent the individual transactions. The transactions are cryptographically hashed and stored on the leaf nodes of the tree as Ha, Hb, Hc and so on. The hash of the child nodes are concatenated and a new root hash is generated. The final root hash (e.g., H1 and H2) is stored on the blockchain. Just the root hash can be verified in order to make sure that all the transactions associated with that root hash are secure and have not been tampered with. Even if a single transaction is changed, all the hash values on that particular side of the tree will change.

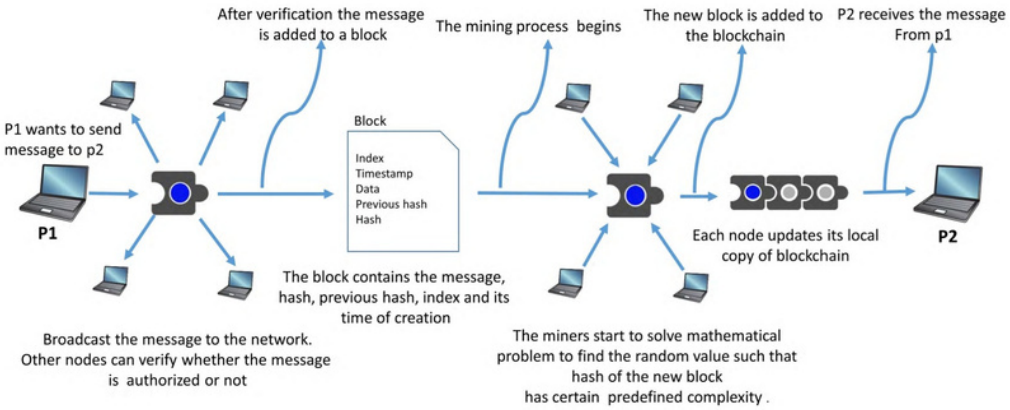


FIGURE 5. Working process of blockchain.

The miners do not have any personal interest in the transactions, and they are mining just to earn their incentives. The miners do not know the identity of the owners of the transactions. Over and above, there are multiple miners working on the same set of transactions, and there is a strong competition between them to add the transactions to the blockchain. All these unique features empower the blockchain to be a strong, tamper-proof, distributed and open data structure for IoT data. Figure shows the complete flow of a transaction from being initialized to being committed to the distributed chain.

- # IoT SECURITY USING FOG COMPUTING

IoT and cloud computing are two independent technologies which have many applications. IoT has provided users with large number of smart devices and applications. Similarly,a cloud provides a very effective solution to store and managedata which can be accessed from anywhere and is widely used by many organizations. IoT is generating an unprecedented amount of data, which puts a lot of strain on the Internetinfrastructure. The integration of cloud and IoT has introduced an era of new opportunities and challenges for processing,storing, managing and securing data more effectively.Industry and research groups have tried to solve some issues faced by the IoT by integrating it with the cloud. The benefits of this integration are not enough to address all the issuesfaced by IoT. Therefore, the concept of fog computing was introduced by Cisco in 2012. Fog computing complements cloud computing rather than replacing it.

• IoT SECURITY USING MACHINE LEARNING

The area of machine learning (ML) has attracted significant interest over recent years. Many domains are using ML for their development, and it is being used for IoT security as well. ML appears to be a promising solution to protectIoT devices against cyber attacks by providing a different approach for defending against attacks as compared to other traditional methods.

The fundamental need in IoT is to secure all the systems and devices that are connected to the network. The role of ML is to use and train algorithms to detect anomalies in IoT devices or to detect any unwanted activity taking place in IoT system to prevent data loss or other issues. Therefore, ML provides a promising platform to overcome the difficulties faced in securing IoT devices. Further contributions in this field are required to maintain the growth of IoT.

- # IoT SECURITY USING EDGE COMPUTING

Edge computing architecture consists of edge devices, cloud server and fog nodes as shown in Figure.
In an edge computing framework the computation and analysis power is provided at the edge itself. The devices in an application can create a network among themselves and can cooperate among each other to compute the data .Consequently, a lot of data can be saved from going outside the device, either to cloud or to fog nodes, and this can enhance the security of the IoT application. Edge computing also helps in providing low communication cost by preventing the need of moving all the data to the cloud traditional methods.

The fundamental need in IoT is to secure all the systems and devices that are connected to the network. The role of ML is to use and train algorithms to detect anomalies in IoT devices or to detect any unwanted activity taking place in IoT system to prevent data loss or other issues. Therefore, ML provides a promising platform to overcome the difficulties faced in securing IoT devices. Further contributions in thisfield are required to maintain the growth of IoT.Edge and fog computing are both extensions of cloud computing which is widely used by various organizations. Cloud, fog and edge may appear similar but they constitute different layers of IoT applications. The main difference between cloud, fog and edge computing is the location of intelligence and power computation.Edge computing architecture consists of edge devices, cloud server and fog nodes as shown in Figure

In an edge computing framework the computation and analysis power is provided at the edge itself. The devices in an application can create a network among themselves andcan cooperate among each other to compute the data.Consequently, a lot of data can be saved from going outsidethe device, either to cloud or to fog nodes, and this can enhance the security of the IoT application. Edge computingalso helps in providing low communication cost by preventing the need of moving all the data to the cloud.

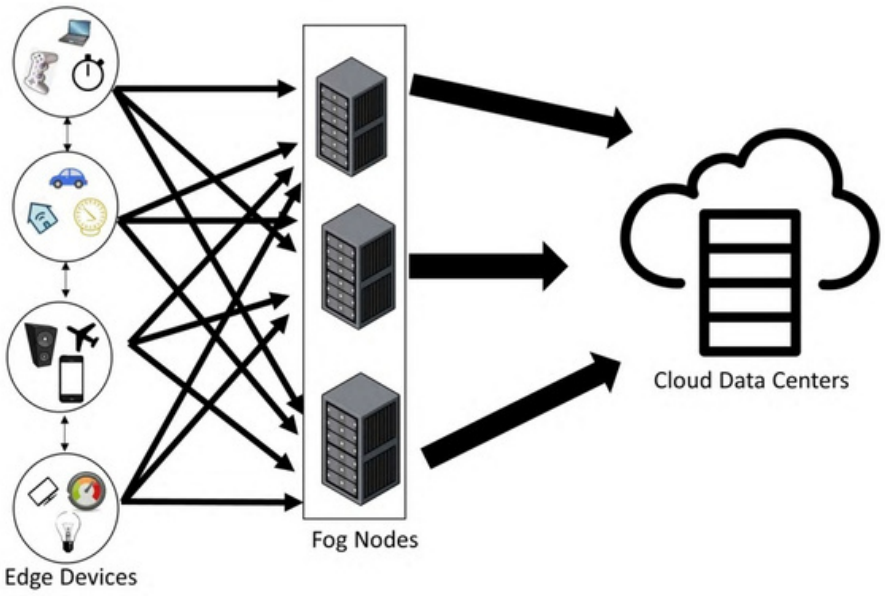


FIGURE 8. Edge computing architecture.

References

1.https://www.researchgate.net/publication/333909259_A_Survey_on_IoT_Security_Application_Areas_Security_Threats_and_Solution_Architectures

2. T. M. Fernández-Caramés and P. Fraga-Lamas, ‘‘A review on the use of blockchain for the Internet of Things,’’ IEEE Access, vol. 6,pp. 32979–33001, 2018.

3.https://www.researchgate.net/publication/350827558_Emerging_Security_Threats_Countermeasures_Issues_and_Future_Aspects_on_the_Internet_of_Things_IoT_A_Systematic_Literature_Review

4. https://sites.google.com/site/tictecbell/Arduino/ultrasons/

5. A. Mosenia and N. K. Jha, ‘‘A comprehensive study of security of nternet-of-Things,’’ IEEE Trans. Emerg. Topics Comput., vol. 5, no. 4,pp. 586–602, Dec. 2017.

6.https://ieeexplore.ieee.org/ielaam/6488907/8709863/8386824-aam.pdf