IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

SECURITY TRENDS IN INTERNET OF THINGS

Kajal Singh
Department of CSE
Lovely Professional University
Phagwara, Punjab, India

Vanapalli Jireesh
Department of CSE
Lovely Professional University
Phagwara, Punjab, India

Mr. Manpreet Singh
Department of CSE
Lovely Professional University
Phagwara, Punjab, India

Anupam Sonkar
Department of CSE
Lovely Professional University
Phagwara, Punjab, India

ABSTRACT:

Internet of Things (IoT) is a network of embedded devices that can be viewed differently and have the embedded software required for communication between interim regions. The purpose of this study was to examine the various IoT security challenges associated with it Standards and IoT agreements currently in place. I have presented a detailed update with details of the IoT structure in the processes and standards given by the next IoT model programs. This research paper aimed to provide more information about IoT security. Since By 2019, IoT, which was operating in smaller network areas, has expanded to a wider area

networks therefore have associated risks due to the expected surgery on IoT devices in diverse environment. This research paper provides insight into the latest security research trends, which will appear to be beneficial to the development of IoT security. Research paper results can benefit the research community in IoT by combining the best security of Io-based devices features.

KEYWORDS: IoT, Security, Blockchain, IOTX, IOTA, Privacy, Ledger,

1 INTRODUCTION

This paper provides insight into the latest trends in security research, which will prove to be beneficial in the development of IoT security. Research findings can benefit the research community IoT by integrating the advanced security features of Io-based devices. The main goal of IoT is the conversion of Internet-enabled devices into a connected ecosystem with accessible digital data anywhere and anytime. IoT security has attracted significant attention in the field of education. Most of the available surveys have investigated relevant security features such as attacks, requirements, and challenges in IoT. However, various emerging technologies and techniques have become more recent has been adopted as a promising solution to improve IoT security. The main purpose of this research paper is to provide the latest updates on current research topics related to IoT security.

2 LITERATURE REVIEW

2.1 IOT

Wireless network with embedded communication is the current course of Industry worldwide. IoT is one of the major beneficiaries of this network domain. IoT Commerce sectors have seen significant growth in the market over the past few years, as a smart plan demand has grown significantly due to its rich feature and one-click services. Intelligent systems as Smart Home machines, AI-based smart devices, smart home automation, smart cars, smart labs, etc., offer easy life but too much reliability on them often leads to serious risks.

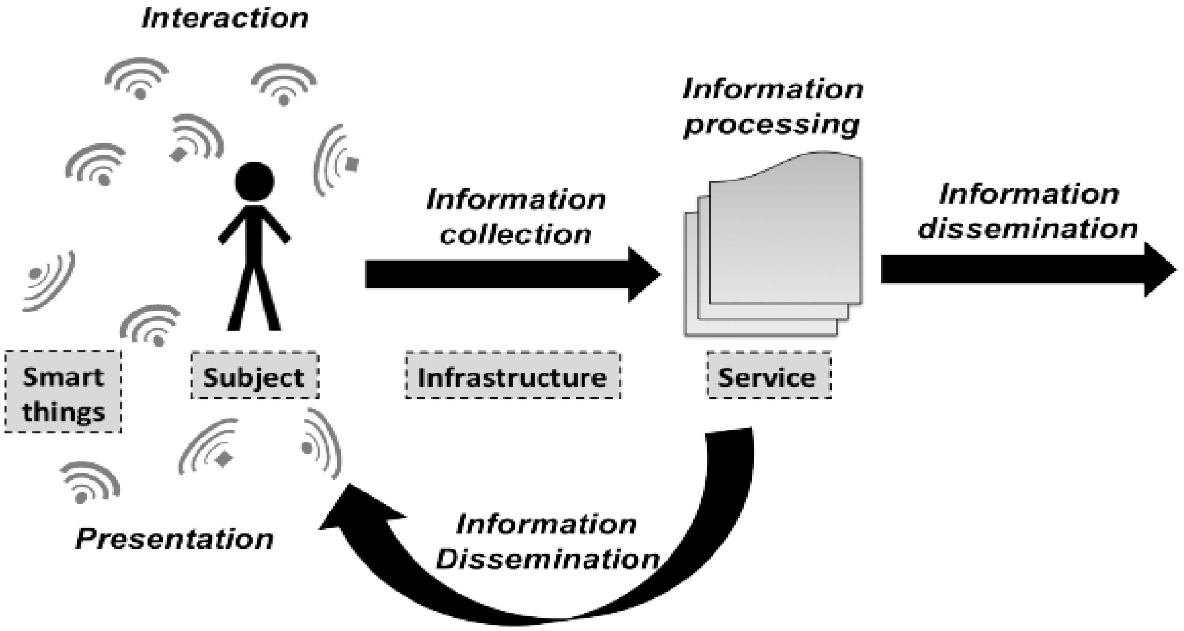

Fig 1 Dataflow in an IOT system

2.2 LITERATURE SURVEY

The latest online concept of Things will go beyond the various components of all of them individual health, which will allow your devices soon. This is from your refrigerators to your thermostats, to make you feel smart, and allow you to connect with different people too things to satisfy their duties. But we cannot deny the fact that we need to have an organized meeting is the background and function of all these devices to communicate with others, and that that is where IOTA will come from.

3 SECURITY FEATURES OF IOT

IoT security challenges can be broadly divided into two classes; Technology and Security opposition. Technological challenges come as a result of the diversity and breadth of IoT devices, while security breach is related to ethics and the assistance to which it should be applied find a secure network. Security should be included in IoT for all growth and performance life cycle of all IoT devices and harps. Below are some safety precautions to be taken access a secure framework for interacting with people, software, processes, and objects on the IoT.

CONFIDENTIAL - It is important to ensure that the data is secure and available only to authorized users.

INTEGRITY - IoT is based on the exchange of data and information between many different types of devices, which is why it is important to ensure data accuracy; that data comes from it correct sender and make sure data is not corrected during the process transfer due to intentional or unintentional disruption.

DISCOVERY - The idea of IoT is to join as many smart devices as possible. IoT users all data should be displayed whenever needed. However, data is not the only module that used in IoT; Devices and services should also be accessible and accessible when needed fashion in time to achieve IoT predictions

VERIFICATION - Each item in the IoT must be smart to clearly identify and validate the Other things. However, this process can be tested due to the nature of IoT; many Organizations are mixed top (devices, people, services, service providers and processing units). In addition, sometimes things may need to interact with other objects for the first time (Things they do not know). Because in all of this, ways to ensure equitable business across all IoT communications.

LIGHTWEIGHT SOLUTIONS - All pre-conceived security targets are rare on IoT, though it may add special features and barriers to all. However, in most cases confidentiality, integrity, disclosure and assurance are considered the primary purpose of everything computer or network security.

HETEROGENEITY - IoT connects different businesses with comparable power, complexity, and vendors. Devices with expired dates and release versions, use deprecated technology interfaces and bitrates, and is designed for different functions. So, the obligations must be defined in order to work on different devices and in different contexts. IoT aims to connect device to device, person to device, and to person to person, thus using communication between different objects and networks. Another challenge to consider in IoT is that environment is constantly changing (dynamics), at the same time the device may be fully connected a different set of devices than ever. Also ensure proper security of the cryptography system required for managing adequate key and security policies.

PRINCIPLES - There must be policies and standards to ensure that data is managed, protected, and is distributed effectively, but more importantly a way to achieve this is needed ensuring that the entire organization applies standards. Service Level Agreements (SLO) should be clearly identified in all services involved. The use of such guidelines will commend trust by human users in the IoT model that will lead to its growth and scalability.

4 SECURITY ISSUES:

The technical report suggests that IoT devices have become a new source of entry-level operations for cyber criminals as there are agreements and standards for these devices are very simple protocols and, on the other hand, build businesses have easy access to the server. These poses challenges to the technology as there is no appropriate final security adjustment. It is recognized that the formation of the threat is not limited to a specific layer in IoT formation. Previous network practices to integrate network security features into IoT have reduced / decreased IoT program performance includes a collection of the latest novels proposed due to the advanced threat reports IoT medicine. Define a security parameter for a specific study function provides a security model related to standard security models. Normal model the issue was Inter-Compatibility among the protection tools installed on IoT devices as they differed from Policy and strategies for use and lack of Low Power device algorithms.

Recent research proposed novel solutions using a wide range of encryption and hardware-based methods ways to overcome common security issues discuss some of these important security issues research models currently.

5 SECURITY SOLUTIONS

The latest IoT security solutions are highly targeted Software-based security measures are more common than conventional one's safety, which focused on tools. Assurance, trust, and the integrity of the communication channel between IoT important security parameters devices relate which are the modern solutions in question. Although still in at present, IoT does not support high-powered devices and it is not consistent enough to deal with the growth of various businesses.

USING BLOCKCHAIN: From the past few years blockchain technology is evolving so rapidly because of its features to provide security and almost impossible to hack. It also provides faster transactions within seconds and it is completely decentralized anyone can use it. And using this technology Bitcoin, Ethereum and many other value crypto coins were created. IOTX, IOTA are also a crypto project based on IOT which was created by using blockchain technology

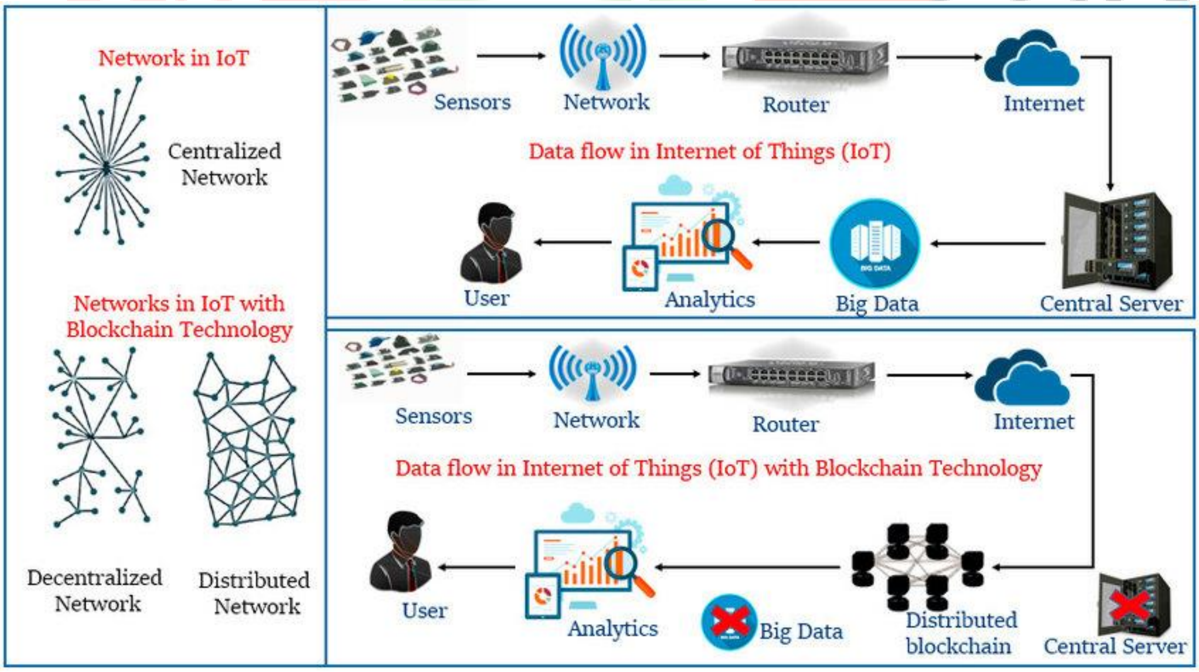

Fig 2, IoT network types, data flow in IoT, data flow in IoT with blockchain technology

5.1 FUTURE OF IOT WITH IOTX:

IOTX is an Ethereum token that enables IoTeX, a platform that aims to connect IoT devices (Such as cameras, sensors, and other devices connected to the Internet) and segmented applications. Today IoT devices are emerging rapidly and are expected to grow to 18 billion devices in 2022. However, most IoT platforms today are medium, unparalleled, four high operating costs, and have concerns related to privacy. As smart IoT devices have changed the way people working together in today's world, IoTeX aims to create an ecosystem were people and devices (machines) can work together using their free will, without worrying about security or rely on and enjoy economic benefits. Smart devices have made data sharing easier and immediately. IoTeX wants to build a platform were businesses and individuals can own it devices and create value from their data.

IoTeX contains two main layers of technology:

Blockchain: According to the platform, the IoTex blockchain is one of the fastest blockchains industry. The IoTex blockchain can complete a block within five seconds compared to the industry an average of 17.49 seconds. The court ruled that their blockchain was operating without error from 2019.

Decentralized Identity (DID): On the other hand, where traditional forums create shared ownership just for humans, IoTex is old-fashioned for people and devices. These symbols work together, as measured in the universe. Using same technique, IoTeX eager to create seamless designs communication between humans and machines.

As IoTeX provides ownership to devices, both individuals and devices can pay as well to charge for services. At IoTeX, even machines are equipped with wallets and smart contracts that do what is done. Wise contracts are like regular contracts; However, smart contracts are there using blockchain-based protocols instead of paper.

5.2 PRIVACY AWARE IOTA LEDGER

IOTA is one of the cryptocurrency tokens which is a blockchain technology solution and Internet of Things. The IOTA blockchain will make all your interactions possible among IoT devices, which will help you speed up IoT adoption across the country the earth. As a user, you can create your own IOTA transaction without any fees.

One of the great things you can find in IOTA is that it will allow you to make your own active or offline. Even if that IOTA is in the development phase and is not yet fully prepared to be used on a large scale, has been included in the top ten crypto currency.

5.2.2 WHAT DOES IOTA BRING TO IOT?

IOTA is a widely distributed ledger in the Internet-of-Things (IoT) industry.

The protocol separates itself from the existing distributed layouts in a structured way acyclic graph. To enable small transactions on smart devices, it uses a measurement method network growth and performance assurance. As the book is still being distributed by the public, what is done in the ledger is completely visible which is why it opens up opportunities for that linking and identification attacks.

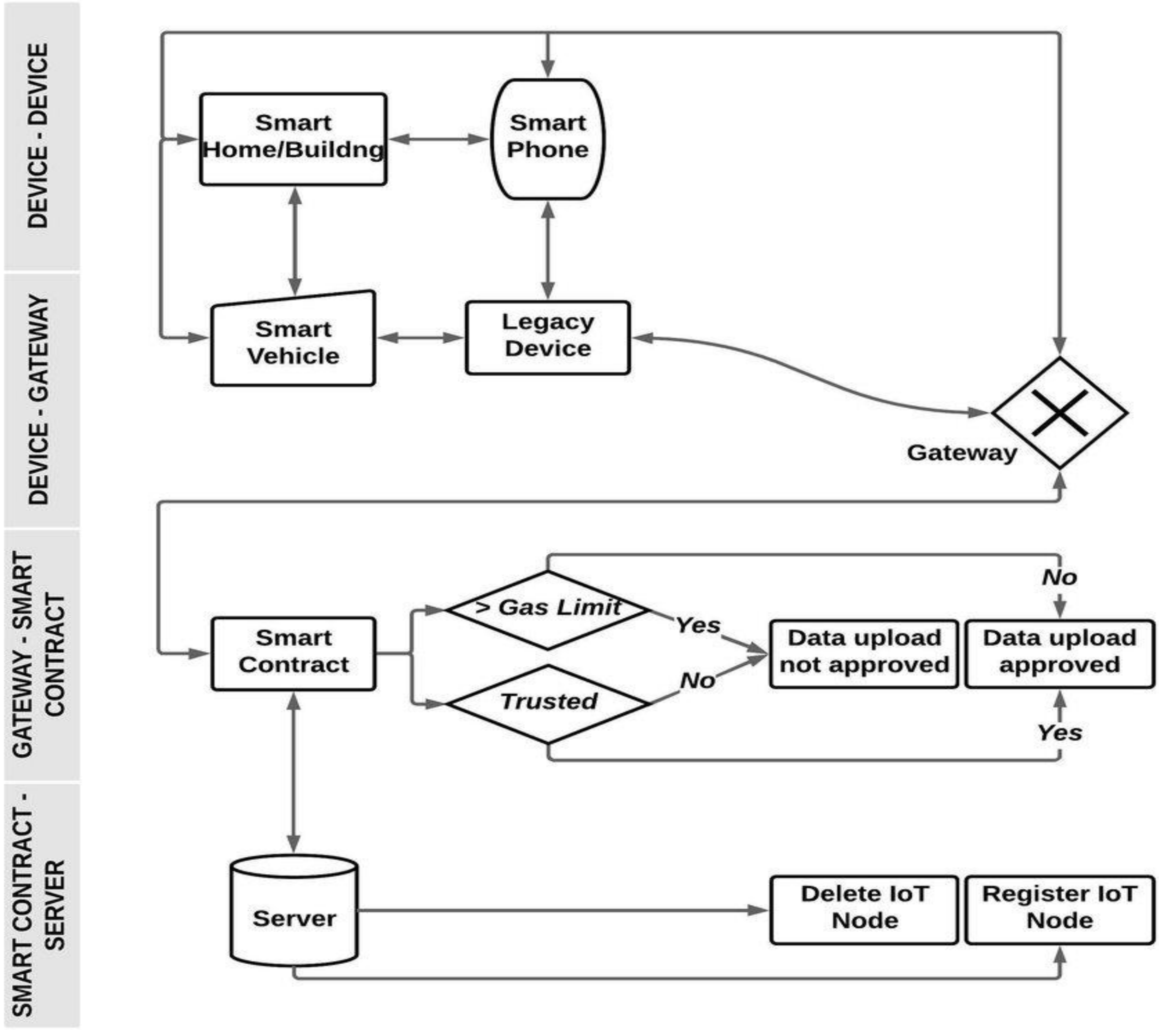

Fig 3 Flow diagram of the IoT Blockchain network

There are four distinct ways to improve privacy is proposed to improve anonymity in distributed layouts. However, many of them proposed methods provide only security guarantees against Elliptic Curve Digital Signature Schemes (ECDSA) and thus do not comply with the IOTA ledger because IOTA uses strong hash-based signatures. Although intermediate solutions are still possible work with IOTA ledger to improve privacy, they are still owners and tend to be single point of failure. We propose a mixing protocol separated from that IOTA ledger novel includes a combination of decryption combinations and multiple signatures. Our strategy does not require a third party (trusted or accountable) and is fully compliant with IOTA Protocol. Analysis of our results for this process shows that security and privacy are not guaranteed even when there are malicious organizations in the system.

Our approach provides strong privacy for the IOTA manual and an added, secure level of

anonymity businesses against identifying and linking attacks.

6 CONCLUSION

The IoT framework is vulnerable to attack on each layer. Therefore, there are many security threats and requirements that need to be submitted. The current state of research in IoT is very focused on protocols to verify and control access, but with the rapid growth of technology is essential integrating new communication protocols such as IPv6 and 5G to achieve continuous integration of IoT topology. Significant development based on IoT especially on a small scale including internally companies and other limited industries. Measuring IoT formation from one company to a discipline for different companies and different systems, different security interests need to be addressed. IoT there are many opportunities for us to change the way we live today. But, the main discipline in awareness absolutely intelligent structures is security. If security commands as privacy, keeping it private, authentication, access control, security protection, trust management, international policies and standards are fully deployed, then all IoT conversions can be done soon future. There is a need for new, wireless diagnostics, software, and hardware technology to resolve it research threats currently open to IoT as standards for different devices, implementation of important management systems and ownership establishments, as well as trust management abilities.

IoT security risks emphasize expansion of IoT threats and IoT threats risk of attack based on protocols and data, highlighting the fact that it is common the methods are no longer as efficient as they used to be against the most common dynamic attacks different IoT environments such as malicious node, DDoS attacks, and botnet attacks. Investigation of modern research models show that most safety solutions are sought through meaning other types of encryption methods, which have been shown to be effective in protection areas of IoT communication channel attacks and promoting low power consumption in process. Integration of technologies such as machine learning, artificial intelligence based on artificial intelligence methods, elliptical cryptographic functions, and blockchain have helped to strengthen the security of IoT networks. On the negative side, it has increased the complexity of the whole system. Due to the high level of production of such complex solutions, transparent for the purpose of security provisions are down. In this work, efforts are being made to address the emergence of existing communication technologies, standards, and internationally accepted standards, endless efforts made (and made) by scientific researchers around the world the topics discussed earlier. However, there is always a range of experiments.

REFERENCES

[1] Security trends in Internet of Things: a survey Rachit1 Shobha Bhatt1 Prakash Rao Ragiri

[2] Ashton K (2009) That Internet of Things thing. RFID J 22:97–114

[3] IoTeX: Took reference from their main website

[4] https://iotex.io/

[5] IOTA: https://www.iota.org/

[6] Coinmarketcap: It's a website that shows live coin prices and information about several crypto projects based on blockchain technologies

[7] https://coinmarketcap.com/currencies/iotex/

[8] https://coinmarketcap.com/currencies/iota/

[9] Salim MM, Rathore S, Park JH (2019) Distributed denial of service attacks and its defences in IoT: a survey. J Supercomputer

[10] Fig 1: https://www.researchgate.net/figure/Data-flow-in-an-IoT-system_fig1_326226121

[11] Fig 2: https://www.researchgate.net/figure/IoT-network-types-data-flow-in-IoT-data-flow-in-IoT-with-blockchain-technology_fig2_325661355

[12] https:// doi.org/10.1007/s11227-019-02945-z

[13] Fig 3: https://www.researchgate.net/figure/Flow-diagram-of-the-IoT-Blockchain-network_fig4_325430814