IJARST
International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

TRANSFORMING IOT DATA SECURITY WITH BLOCKCHAIN TECHNOLOGY

[1]L.PRIYANKA, [2]PANJALA SRUJAN

[1]Assistant Professor, Depatment Of MCA, Sree Chaitanya College of Engineering, Karimnagar

[2]MCA Student, Depatment Of MCA, Sree Chaitanya College of Engineering, Karimnagar

ABSTRACT:

Although the Internet of Things (IoT) is still in its infancy, it will eventually have an impact on practically every object we use on a daily basis. The likelihood of it being abused will increase with its integration into our daily lives. Making IoT devices safe against cracking is urgently needed. In the near future, IoT will increase the scope of cyberattacks on households and companies by turning offline devices into online systems. Simply said, current security solutions are insufficient to address this issue. In the future, blockchain technology may be used to build more secure Internet of Things systems. This article first provides an introduction of blockchain technology and its implementation, then discusses the IoT architecture, which is built on a blockchain network, and last offers a model for internet of things security using blockchain.

I. INTRODUCTION

Software scientists have been too interested in blockchain technology since its inception. Fig. 1 illustrates the foundations of blockchain technology in the internet realm. In actuality, it has the capacity to totally revamp and enhance the global network of internet-connected technology. It will significantly affect two areas: First of all, by creating a decentralised system, it does away with the convenience of central servers and makes peer-to-peer communication possible. Secondly, it can create a completely transparent database that is open to the public, which might make elections and government more transparent. The first of the four core pillars of blockchain technology is consensus, which provides proof of work (PoW) and verifies network activity. The second is the ledger, which provides detailed transaction records inside networks. The third is cryptography, which guarantees that all information in ledgers and networks is encrypted and could only be decoded by authorised users. The fourth is the use of smart contracts for network member authentication and confirmation. IoT is expanding quickly and gaining traction in almost every technical field. Its rapid expansion, however, has made it more susceptible to hackers. IoT security has to be improved immediately [1].

The Internet of Things (IoT) is a loosely connected system made up of a number of homogeneous and heterogeneous devices having computing, network, and sensor capabilities [2]. The Internet of Things has been suitably and semantically defined by the IoT vision [3].The best approach to keep your car safe and secure right now is to lock it, either manually or automatically. We become more assured of its safety and security [4]. In the future, every piece of equipment in our cars will be sensor-based and incorporated into the system at the same time [5]. Our cars are smarter thanks to these devices, but are they safe? To answer this crucial question, we need to create a more secure architecture that will enable our

Internet of Things-based cars to be safe, secure, and constantly connected to the Internet [6]. In order to develop a more dependable and secure Internet of Things paradigm, this research paper aims to provide examples and recommendations for the use of blockchain technology. To make our essay more clear, we go into further depth in the next section VI. Section II discusses the need for security in the Internet of Things environment, Section III introduces blockchain technology, and Section IV explains the architecture of the blockchain-based Internet of Things. Section V illustrates the security benefits of the blockchain for IoT architecture. Our essay has come to a close in Section VI.

II. LITERATURE SURVEY

A survey of Internet-of- Things: Future vision, architecture, challenges and services

Internet-of-Things (IoT) is the convergence of Internet with RFID, Sensor and smart objects. IoT can be defined as "things belonging to the Internet" to supply and access all of real-world information. Billions of devices are expected to be associated into the system and that shall require huge distribution of networks as well as the process of transforming raw data into meaningful inferences. IoT is the biggest promise of the technology today, but still lacking a novel mechanism, which can be perceived through the lenses of Internet, things and semantic vision. This paper presents a novel architecture model for IoT with the help of Semantic Fusion Model (SFM). This architecture introduces the use of Smart Semantic framework to encapsulate the processed information from sensor networks. The smart embedded system is having semantic logic and semantic value based Information to make the system an intelligent system. This paper presents a discussion on Internet oriented applications, services, visual aspect and challenges for Internet of things using RFID, 6lowpan and sensor networks.

Cyber-Physical Systems Security-A Survey

With the exponential growth of cyber-physical systems (CPSs), new security challenges have emerged. Various vulnerabilities, threats, attacks, and controls have been introduced for the new generation of CPS. However, there lacks a systematic review of the CPS security literature. In particular, the heterogeneity of CPS components and the diversity of CPS systems have made it difficult to study the problem with one generalized model. In this paper, we study and systematize existing research on CPS security under a unified framework. The framework consists of three orthogonal coordinates: 1) from the security perspective, we follow the well-known taxonomy of threats, vulnerabilities, attacks and controls; 2) from the CPS components perspective, we focus on cyber, physical, and cyberphysical components; and 3) from the CPS systems perspective, we explore general CPS features as well as representative systems (e.g., smart grids, medical CPS, and smart cars). The model can be both abstract to show general interactions of components in a CPS application, and specific to capture any details when needed. By doing so, we aim to build a model that is abstract enough to be applicable to various heterogeneous CPS applications; and to gain a modular view of the tightly coupled CPS components. Such abstract decoupling makes it possible to gain a systematic understanding of CPS security, and to highlight the potential sources of attacks and ways of protection. With this intensive literature review, we attempt to summarize the state-of-the-art on CPS security, provide researchers with a comprehensive list of references, and also encourage the audience to further explore this emerging field.

Radar Sensors in Cars." in Automated Driving, Springer International Publishing

In recent years, Cloud Computing and Internet of Things (IoT) have been rapidly advancing as the two fundamental technologies of the Future Internet (FI) concept. Different IoT systems are designed and implemented according to the IoT domain requirements, thus not taking into consideration issues of openness, scalability, interoperability, and use case independence. This work focuses on the presentation of a framework that integrates future IoT systems in smart cities by utilizing state-of-the-art architectures, technologies, solutions, and services developed by the IoT-A and FIWARE FP7 projects of the EU. We expect that in future smart city environments, an IoT infrastructure will act as a key enabler for the revolution of smart networked systems with embedded devices. Also, the proposed solution overcomes the fragmentation of vertically oriented closed systems, architectures, and application areas and move towards open systems and platforms that support multiple applications. This is a key requirement for smart city infrastructures that can be reused by a plethora of applications in various domains, such as transportation systems, energy, waste management, environmental monitoring, buildings, etc. The proposed system will encompass FIWARE and IoT-A to develop innovative IoT platforms and services and it will include generic IoT devices that are independent of connectivity modes and are not coupled to specific IoT protocols. It will further supply interoperability with emerging connectivity protocols based on actions regarding standardization and requirements. We expect that future solutions will simplify data transfer by supporting the vast majority of transfer protocols and will allow effective utilization of network capabilities for transition and reception of real-time data. Using FIWARE services will ensure reliability, modularity, and uniform APIs independent of the underlying hardware and it will move beyond current solutions that are platform dependent, and vendor specific. The result will be a dynamic configurable infrastructure, scalable, interoperable, heterogeneous, and secure that could also seamlessly integrate other existing and future platforms and devices. Information can flow among IoT systems in a secure and privacy-preserving way, allowing for extracting context for developing cross-domain applications and breaking the domain silos of today’s IoT world.

The internet of things: A survey

This paper addresses the Internet of Things. Main enabling factor of this promising paradigm is the integration of several technologies and communications solutions. Identification and tracking technologies, wired and wireless sensor and actuator networks, enhanced communication protocols (shared with the Next Generation Internet), and distributed intelligence for smart objects are just the most relevant. As one can easily imagine, any serious contribution to the advance of the Internet of Things must necessarily be the result of synergetic activities conducted in different fields of knowledge, such as telecommunications, informatics, electronics and social science. In such a complex scenario, this survey is directed to those who want to approach this complex discipline and contribute to its development. Different visions of this Internet of Things paradigm are reported and enabling technologies reviewed. What emerges is that still major issues shall be faced by the research community. The most relevant among them are addressed in details.

III. SYSTEM ANALYSIS AND DESIGN

EXISTING SYSTEM:

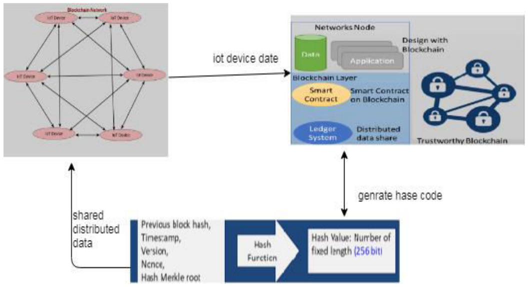
Blockchain technology is now getting too much of attention from software scientists since it has been cre- ated. Fig 1 shows the basic pillars of blockchain technology in internet world. Actually, it has the ability to revolutionize and optimize the global infrastructure of the technologies connected with each other through internet. It has mainly two fields that are going to be influenced by it which are: By creating a decentralized system, it removes the indulgence of central servers and provides peer-to-peer interaction. It can create a fully transparent and open to all database, which could bring transparency to the governance and elections. Blockchain technology basically has 4 pillars, first, Consensus, which provides the proof of work (PoW) and verifies the action in the networks, second is ledger, which provides the complete details of transaction within networks. Third, Cryptography, it makes sure that all data in ledger and networks gets encrypted and only authorized user can decrypt the information and fourth is smart contract, it is used to verify and validate the participants of the network.

PROPOSED SYSTEM:

The purpose of this research paper is to provide guidance for the use of blockchain technology, through cases to make a more secure and trustable IoT model IoT has numerous applications, for example: in making smart homes, Smart City, Improving Health, Autonomous Vehicles, etc. Some IoT devices are currently available in the market like Wearables, Smart Thermostat Systems, Air Conditioners, and refrigerators that use Wi-Fi for remote monitoring. Apart from all these benefits, IoT has some serious issues, which should be sorted out before it gets implemented, like the technologies on which the foundations of IoT have been established have several bugs, so if hackers get access to the system through these bugs then they can compromise the privacy of the customer or even can cause harm to them. Thus before implementing IoT, the security of these systems should be strengthened and made free from any bugs. Keeping the IoT device secure is one of the most difficult tasks to accomplish. In making these devices cheap, small and easy to use many security policies are compromised which increases the risk of security breach.

IV. SYSTEM DESIGN

SYSTEM ARCHITECTURE



V. SYSTEM IMPLEMENTATION

MODULES:

1. **Network of Nodes**:
 All the nodes connected through the internet maintain all of the transactions made on a blockchain network collaboratively. The authenticity of the transaction is checked by the protocol, which eliminates the involvement of a trusted third party for validation purpose . When a transaction is done, its records are added to the ledger of past transaction, this process is known as 'mining'. The proof of work has to be verified by the other nodes present on the network.
2. **Distributed database system:**
 The database, which is composed of blocks of information, is copied to every node of the system. Each block contains the following data in itself: A list of transactions; a timestamp; Information, which links it to the previous chain of the blocks.
3. **Shared ledger:**
The ledger is updated every time a transaction is made. It is publicly available and is incorruptible which introduces transparency to the system.
4. **Cryptography:**
It binds the data with the very strong crypto mechanism, which is not easy to track or tampered by unauthorized users.

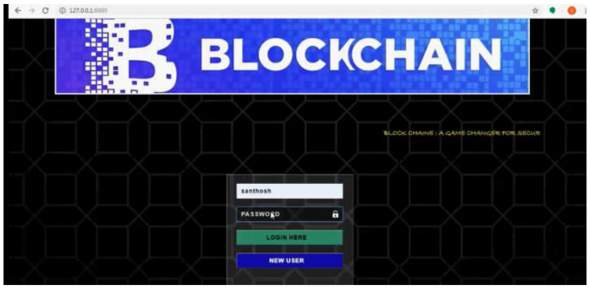
VI. ALGORITHM:

Block chain Technique:

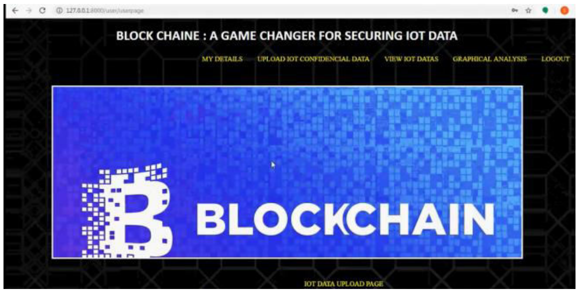
A blockchain, originally block chain, is a growing list of records, called blocks, which are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. By design, a blockchain is resistant to modification of the data.

The emergence and popularity of blockchain techniques will significantly change the way of digital system operation and management. Blockchain is essentially a digital public ledger that securely records and automatically verifies high volume transactions digitally. By allowing digital information to be distributed, blockchain technology created the backbone of a new type of internet.Originally devised for the digital currency, Bitcoin, the tech community is now finding other potential uses for the technology. The application of blockchain will exhibit a variety of complicated problems and new requirements, which brings more open issues and challenges for research communities.

VII. SCREEN SHOTS



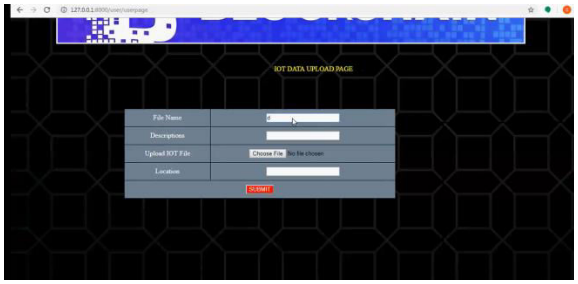
santhosh



127.0.0.1:8000/user/userpage

BLOCK CHAINE : A GAME CHANGER FOR SECURING IOT DATA

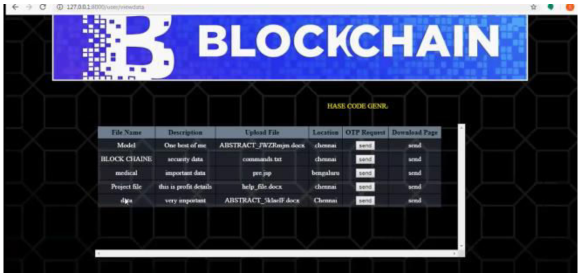
IOT DATA UPLOAD PAGE



127.0.0.1:8000/user/userpage

IOT DATA UPLOAD PAGE

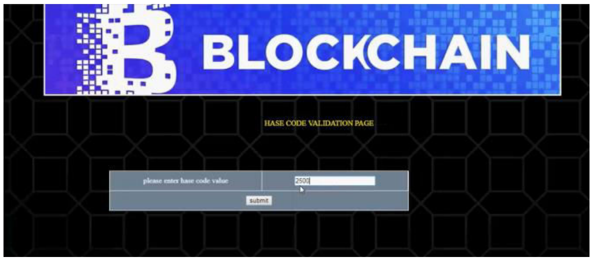
File Name: d
Descriptions:
Upload IOT File: Choose File No file chosen
Location:



127.0.0.1:8000/user/viewdata

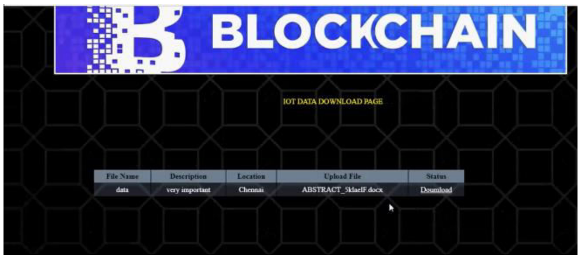
HASE CODE GENR.

File Name	Description	Upload File	Location	OTP Request	Download Page
Model	One best of me	ABSTRACT_JWZRmjm.docx	chennai	send	send
BLOCK CHAINE	security data	commands.txt	chennai	send	send
medical	important data	pre.jsp	bengaluru	send	send
Project file	this is profit details	help_file.docx	chennai	send	send
data	very important	ABSTRACT_5klaelF.docx	Chennai	send	send



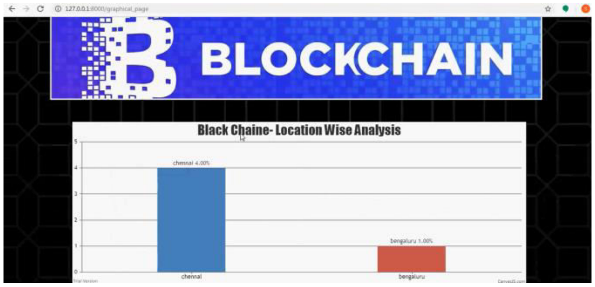
HASE CODE VALIDATION PAGE

please enter hase code value: 2500



IOT DATA DOWNLOAD PAGE

File Name	Description	Location	Upload File	Status
data	very important	Chennai	ABSTRACT_5klaelF.docx	Download



127.0.0.1:8000/graphical_page

VIII. CONCLUSION

This article offers examples and recommendations for using blockchain technology to create a more reliable and secure Internet of Things platform. We came to the conclusion that the internet of things would not be a complete member of a blockchain network due to the high-end hardware requirements. However, the blockchain technology's new features, which are made available through APIs provided by network nodes or other specialised middlemen, will undoubtedly assist the internet of things. The internet of things might be made extremely safe with these features. We have talked about the cybersecurity aspect of the recently developed blockchain technology. Since Bitcoin is a cryptocurrency that is built on blockchain technology, blockchain technology is mostly used and focused on in the banking sector. However, in order to enable safe data transfer between internet-connected devices, we attempt to provide blockchain technology for the internet of things in this essay. For this, we have discussed and offered blockchain as a solution for IoT security, as well as given an overview of blockchain technology and security concerns in the IoT context.

REFERENCES

1. Singh Dhananjay, Gaurav Tripathi and Antonio J. Jara, "A survey of Internet-of- Things: Future vision architecture challenges and services", Internet of Things (WF-IoT), 2014.
2. Atzori and Morabito, "The internet of things: A survey", Computer Networks, vol. 54, no. 15, pp. 2787-2805, 2010.
3. Humayed Abdulmalik, Cyber-Physical Systems Security-A Survey, 2017.
4. Meinel Holger and Wolfgang Bosch, "Radar Sensors in Cars." in Automated Driving, Springer International Publishing, pp. 245-261, 2017.
5. Uden Lorna and Wu He, "How the Internet of Things can help knowledge management: a case study from the automotive domain", Journal of Knowledge Management, vol. 21, no. 1, 2017.
6. Sot iriadis, Stelios, Kostantinos St ravoskoufos and Euripides GM Pet rakis, "Future Internet Systems Design and Implementation: Cloud and IoT Services Based on IoT-A and FIWARE." in Designing Developing and Facilitating Smart Cities, Springer International Publishing, pp. 193-207, 2017.
7. On Public and Private Blockchains, 2017.
8. Madhusudan Singh, "Perspective Challenges and Future of Automotive Security Enriched with Blockchain Technology", IEEE Transportation Electrification Community Webinar-Abstract, Dec 2017.
9. Understanding Autonomous Organizations on the Blockchain.
10. C. Decker and R. Wattenhofer, "A fast and scalable payment network with bitcoin duplex micropayment channels" in Stabilization Safety and Security of Distributed Systems, Springer, pp. 3-18, 2015.
11. Das Manik Lal, "Privacy and Security Challenges in Internet of Things", Distributed Computing andInternet Technology., pp. 33-48, 2015.
12. Joseph Bonneau, "Research Perspectives and Challenges for Bitcoin and Cryptocurrencies", IEEE SECURITY AND PRIVACY (forthcoming May 2015).