Iot Security – A Secure Data Transfer among Iot Nodes

Dwarakanath G V
Research Scholar, Dept. of Computer Science, Marwadi University
Email: dwarakanathgv@bmsit.in
Dr. R Sridaran
Dean Academics and Dean Computer Applications, Marwadi University
Email: sridaran.rajagopal@marwadieducation.edu.in

ABSTRACT

The phrase "IoT" (IoT) designates a concept that encompasses a wide range of object types and communication methods. Today, the term "IoT" is more often used to refer to the notion that everything is accessible online. IoT will be essential in the future since the concept opens up the door for additional services and advancements. Since they continue operating in unprotected exterior, all products will be intertwined and allowed to converse with one another. This latter element causes significant security issues.

Today's Internet of Things (IoT) requires a standardized and transparent architecture that outlines how well this innovation should be used when IoT devices should safely communicate with one another. The methods used by technology to collect and process data are at the core of the security problems. The Iot is introduced in this thesis along with some potential applications and information security concerns. The thesis also provides some suggestions for potential fixes to the basic issues with identification and secure communications. The offered solutions are built on both the newest technology and that which is still in development. Modern solutions are constructed upon security measures like IPSec and DTLS. These protocols are used in a context that includes the Web and a 6LoWPAN network. The proposed authentication method is built on the open vital infrastructures and certificate management trust models.

The paper lists various areas in which this theory may be applied for additional research. These areas of competence include additional vulnerability assessments and deployment of the indicated fixes.

Keywords – **Authentication, Communication, Internet of Things (IoT), Identifications, Information Security.**

I. INTRODUCTION

Due to the general risks and stakes involved, there has been considerable concern regarding data security on a global scale. It's getting more and moresensitive as a result of the Internet of Things and other expanding heterogeneous technical frameworks that allow device-to- device connection. It attempts to make life easier for individuals even while posing new issues that need to be resolved in order to protect information. Several encryption schemes that might have been mentioned in the literature have undergone extensive development in order to protect data or information. One of the various symmetric cryptographic encryption-based data encryption approaches that have been disclosed recently with the use of confusion as well as diffusion processes. Several of the methods use substitution techniques to enhance the encryption quality. AES data encryption algorithms are very unpredictable and sensitive to initial conditions, which has led to their rapid proliferation. So, because control parameters or system parameters of these dynamical systems are taken from the key, this increases their reliance on the key. The binary key is used by many cryptosystems to create subkeys, which are subsequently used to create other parameters. The present endeavor concentrates in AES data encryption to provide information security in IoT devices. A 128-bit key is used to create an initial and control parameter, making it robust enough to fend off a brute - force attacks. The confusion and diffusion properties of the cypher text enhance the encryption's effectiveness. The real - time news key is more important to the cypher text since it is continuously modified together with the integrity for each input block of data. This model should be able to show how valuable it is for devices and systems with small computational footprints.

II. LITERATURE SURVEY

Since the Internet of Things is based on the idea that anything may be connected, interconnectedness is its fundamental attribute. Services for things revolve around how devices' C.P.U., memory, and power limitations limit what they can do, when they can do it, and how frequently they can do it. To ensure semantic coherence A virtual item that aim to determine the temperature among measurements and is mapped to a real thing that records temperatures at regular intervals may report a temperature value that differs from the physical value.

creating a distributed IoT architecture based on a hash chain that manages keys securely. A set of secret keys pairs are sent to the IoT devices by the proposed approach via each hash chain technique, which enables the key pairs to independently verify itself at any moment. Create plans for device and AMN communication thru an inter- network.Implement and

assess the plans to ensure they can meet the needs for performance and security [1]. Proposes a decentralized trust strategy to preserve the standing of fog models that are open to the general public. To enable decentralized trustworthy service provisioning among IoT devices and public fog models, this trust model was developed using the Ethereum blockchain and cryptographic protocol technology. A few minor problems that can be fixed to ensure contracts have been brought to our attention by the tools employed in the present scheme [2]. Here, we have put forth a solution for data attestation that uses entire models as verifiers to vouch for the accuracy of the responses provided by gateway of lite nodes. Since they are unable to independently verify the data from the blockchain network, they have used smart contracts to offer lightweight clients trust in the information reported. Only blockchain-based approaches with the front system are the focus of this article. Decentralized apps will be used to keep the solution decentralised, and as a result, the suggested system will soon be implemented on the primary network [3]. We implement a piece of software based blockchain method for fogs, which serves as a decentralized client-servers network medium, to strengthen data security across IoTs. The 'BFIMs' scheme outperforms the resource deliverables AES, DES, and RSA in terms of throughput and task scheduling capacity. With high latency or inefficient end- to-end data transmission in the cloud, network problems, and allotted shared end devices, cloud computing is a model of on demand delivering computing services that leverages the internet [4]. This study suggests a simple blockchain- based authentication method that stores the credentials of regular sensors. To determine whether there is any malicious node in the predicted route, a route correctness technique is suggested. While a list of rogue nodes is kept in the blockchain or used in the routing integrity mechanism, a detection system is proposed to limit the activities of hostile nodes. Although the proposed approach is economical, processing and transferring/storing data among nodes takes additional time [5]. The key objectives of the suggested system are contact tracing, quick early diagnoses, monitoring systems, alerting, and social distance control. The following tests and information gathered throughout triage comprise the four data types employed in this system:

recordings of coughs, CT scans, and ECG signals.

Due to a paucity of data from previous pandemics, the tracking systems were not fully built, and the teams also rely upon past data from the present pandemic [6]. This study offers a revolutionary decentralized important management architecture (bdkm) built on blockchains, using fog computing to cut latency and several blockchains operating in the cloud to enable pass access. To speed up the verification process and conserve precious storage capacity for Internet of Things (IoT) devices, we divided the network into various side blockchains based on the deployment domain. Key update operations in Blom's and the pre-shared key schemes result in computational overhead for a significant number of additional nodes and cannot be carried outin an uninterrupted pattern. The node engaged in thecore update or the intricacy of each operation are thetwo fundamental factors of the central point cost [7]. Iot keyword cluster, keyword trends, subject categorization, and topic trends are all included in this study for interested academics. The limitations of this study include, for example, the use of article names as keywords during the collection of articles for analysis. Articles that are implicitly about IoT security may therefore be excluded from this analysis. Additional expenditures associated to Blockchain technology exist; it needs a lot of bandwidth and processing power [8]. So that any unauthorized receivers cannot access the system, correct setup of IoT is performed at the physical level in IoT architecture. This paper addresses the four types of IoT attacks: "Physical attack," "Software attack," Network attack," and "Encryption attack" based on vulnerabilities. There are other ways to create blockchain, but in this paper, Gcoin Blockchain is implemented using Consortium proof of work. Every medicine is tracked on the Gcoin Blockchain in the same way that bitcoin is tracked on the Blockchain. These concepts still need to be put into practice. Due to resource limitations, blockchain technology cannot be used by many IoT devices [9]. The proposed architecture's qualitative evaluation focuses on how it responds to different attacks. The IoT ecosystem's nodes may all be uniquely identified thanks to the benefits of addressing provided by blockchain technology. Certain Blockchain assaults can completely shut down the system. Distributed access control has been attempted in a few articles, but the overheads and severe delays were too much for them to handle. IoT networks have a huge number of nodes, and Ethereum scales poorly as the number or nodes in a network increase [10].

III. PROPOSED SYSTEM

This system proposes a new security model for implementing secured IoT system consisting of various nodes. We have researched in a way where we have tried implementing different encryption algorithm at node level of Iot system. We have implemented AES encryption algorithm for encrypting data that is continuously generated from diverse sensors. The main objective of this new security model is to secure the data that are being generated at end- node level of IoT system. Even if this system is compromised, the data will be safe as it would be encrypted and without the knowledge ofadmin, the attackers cannot get access to the data. Since the data will not be compromised at any level,we can say that we have a new security model that can be implemented anywhere to any IoT system.

IV. IMPLEMENTATION

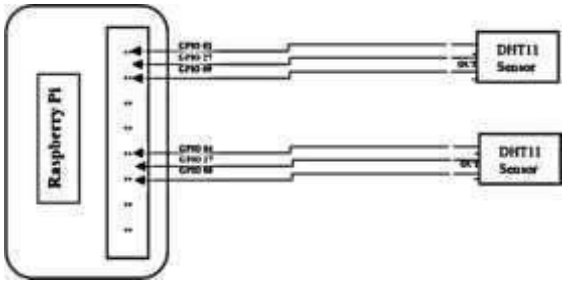
We have tried merging the two major fields in the technology which are Cryptography and IoT to protect the data from being exposed into the outside world. We

have implemented AES encrypting algorithm for the encryption of the voluminous data that is being generated through DHT11 sensor, which is mainly used in our system. This system assures a safe and leak proof data transmission among the IoT nodes.

There some software that needs to be installed first before starting implementing this system. Firstly, we need to take the 32gb SD-card and insert it into the computer system. We need to download the raspberry pi OS into the system. After formatting the SD card once, we need to write that OS onto that SD card. Now insert that SD card to raspberry pi and the system needs a reboot to install the OS. Finally, we are ready with the operating system to work with raspberry pi. This completes the software installation in raspberry pi.

We need another software called VNC, Virtual Network Computing which is used to view and work on raspberry pi on our laptop. We just need to search for VNC viewer software in google web search and need to download to install the software. After installing VNC viewer, we have to specify the IP address of the raspberry pi in order to connect through our laptop. One more thing to remember before connecting, both our laptop and raspberry pi should be connected to same network through ethernet cable; only then we will be able to access the raspberry pi through our laptop.

to GPIO pins of Raspberry pi, the ground pin needs to be connected ground pins in RPi and lastly the power pin



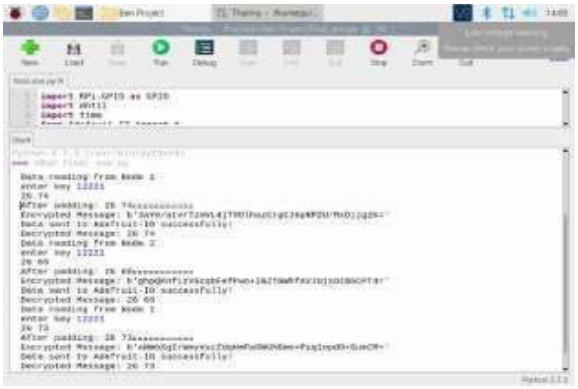
Circuit Diagram

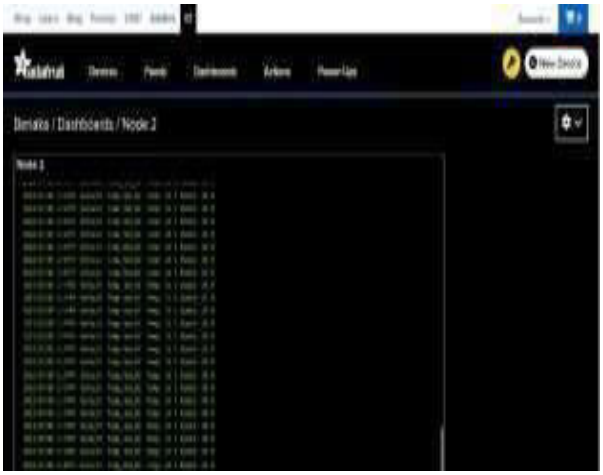
The below diagram represents the circuit diagram of our system, like how the sensors are need to be connected to raspberry pi on which GPIO pins.

DHT11 sensor has three pins; namely: signal pins, ground pins and power pins. The signal pin should be connected

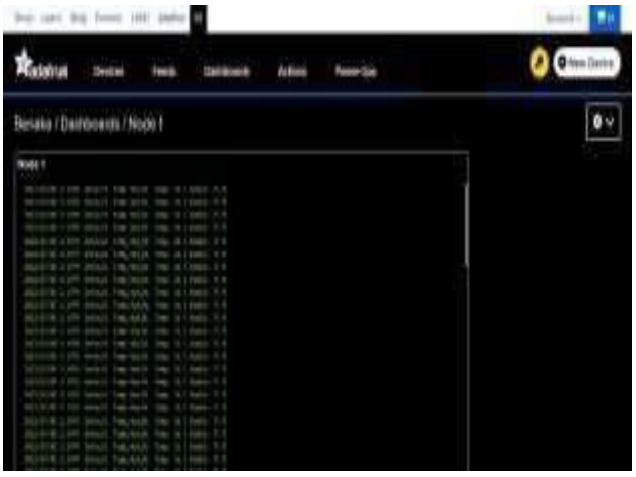
Fig 5.1 Circuit Diagram

Screen Shots





should be connected to VCC pins available in the RPi. Refer the below diagram to keenly obtain the clear picture about the connections.



V. CONCLUSION

In this paper, we have implemented a new IoT security model which is a way more secure and safe in the real world. We have tried merging thetwo major fields in the technology which are Cryptography and IoT to protect the data from being exposed into the outside world. We have implemented AES encrypting algorithm for the encryption of the voluminous data that is being generated through DHT11 sensor, which is mainly used in our system. This system assures a safe and leak proof data transmission among the IoT nodes. Even when the whole system being compromised, the data cannot be compromised by any outsiders/hackers. Finally, we are able to build a new security model to any IoT systems which can be implemented in the real world and yet this finding is just a start to new concept/field IoT security. This security model can be utilized into other projects which a mainly security concerned.

REFERENCES

[1] Xu. Wnagu, Xu. Wangu, Ju. Zhaao, Zu. Zhuang, Chsaotic encsryption aglgorithm based on alternate of streams ands blocsk ciphser, monlinear dynamicss.

[2] EE. Alawarez, Ar. Feernandez, P. Grsacia, J. Jismenez, A. Marcsano, News adpproach to chaotisc esncryption, Phsysics Letterss.

[3] Ku.Wu. Wuong, Ab fasts chaotisc cryptographics schemes with dynamics look-up tables, Phzysics Laetters.

[4] N.K. Pareeks, V.Patidars, K.Ssud, Disscrete chaotics crsyptography usings extsernal key, Physaics Laetters.

[5] Mr. Baptistaa, Cryptographay with chaaos, Physaics Letaters

[6] Mr. Kumara, S. Kumara, R. Budhairaja, M. K. Daas and S. Saingh, Inteartwining logiaastic maap and Cellaular Automata bdased csolor imagse encryptiosn smodel, 2016 Insternational Conferensce on Computsational Teschniqsues in Inforsmation and Cosmmunication Technodlogies(ICCTICT), New Delhi.

[7] N. Pareeask, V. Patidar, K. Susd, Crysptography usindg multiple one-didmensional chaodtic maps, Communicadtions in Nonlidnear Sciencde and Nudmerical Simdulation.d

[8] N. K. Preeak, V. Patidasar, K. K. Saud, Blocak cipsher usinsg 1D anad 2D chaotisc msaps, Internsational Joursnal of Infsormation & Comsmunication Technsology.

[9] Manisha Kumara, Sunil Kumaar, Rajaat Budhiaraja, M.Ka. Das, Saanjeev Siaangh, A cryptographic model baaased on laogistic maap anda 3-D matrix, journaal of informatiaon securiaty and applications.

[10] Md Whaiduzzaman, Md. Julkar Nayeen Mahi, Alistair Barros, Md. Ibrahim Khalil, Colin Fidge, Rajkumar Buyya. "BFIM: Performance Measurement of a Blockchain Based Hierarchical Tree Layered Fog-IoT Microservice Architecture", IEEE Access, 2021

[11] SHAHID ABBAS, NADEEM JAVAID, (Senior Member, IEEE), AHMAD ALMOGREN 2 , (Senior Member, IEEE), SARDAR MUHAMMAD GULFAM, ABRAR AHMED , AND AYMAN RADWAN , (Senior Member, IEEE) “Securing Genetic Algorithm Enabled SDN Routing for Blockchain Based Internet of Things” IEEE Access, 2021.

[12] Farshad Firouzi , Bahar Farahani , Mahmoud Daneshmand , Kathy Grise , Jaeseung Song , Roberto Saracco , Lucy Lu Wang, Kyle Lo, Plamen Angelov , Eduardo Soares, Po-Shen Loh, Zeynab Talebpour “Harnessing the Power of Smart and Connected Health to Tackle COVID-19: IoT, AI, Robotics, and Blockchain for a Better World” IEEE Access, 2021.

[13] Vinay Kumar Calastry Ramesh, Yoohwan Kim, Ju-Yeon Jo. "Secure IoT Data Management in a Private Ethereum Blockchain" , 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC), 2020

[14] Steffi Das, Rithik Richard, Magalaxmi N, Sri Charan, Chaya Ravindra. "Wearable Smart Heart Monitor using IOT" , 2022 IEEE International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE), 2022

[15] "Mobile Computing and Sustainable Informatics" , Springer Science and Business Media LLC, 2022 [12] Yuanxia He, Jinghua Tian, Yujia Cao. "Intelligent home temperature and light