iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** X **Month of publication:** October 2017

DOI: http://doi.org/10.22214/ijraset.2017.10254

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue X, October 2017- Available at www.ijraset.com

Password Protection Using Gödelization Technique for IOT Device

M.V.G Sirisha[1], G.V.Hindumathi[2], Dr.D.Lalitha Bhaskari[3]
[1, 2,3]*Computer Science & Systems Engineering, Andhra University*

Abstract: ***Automation systems are being preferred over manual systems in all aspects in the advancement of Technology. Internet of things over the world occupies a special role to control the Automation devices. Many attacks are found as per the security aspects in Internet of things. This paper is focused about password protection system for detecting the attacks due to minimal security aspects considered. Here Gödelization method is used to protect the password for proper authentication. Gödelization technique gives a new secure number format and it is helpful for validating the password given by the user. The secured number format used by an IoT device is to provide security. An IoT Device which acts like a server accepts the password and verifies it. If it is correct password, then allows Wifi to all clients.***
Keywords*: Internet of Things, Gödelization, Authentication, Security Vulnerabilities, password protection system.*

I. INTRODUCTION

IoT device include thermostats, light bulbs, door locks, fridges, cars etc. These devices are part of a scenario in which every device talks every other related device in an environment to automate home and industry and communicate more and more usable data to users, business and other interested parties. The Internet of things (IoT) is the between systems administration of physical devices, vehicles, buildings, and different things embedded with hardware, programming, sensors, actuators, and system availability which empowers as shown in figure 1. These devices gathers information and exchange information. IoT is required to offer advanced network of devices, frameworks and uses multiple protocols, domains, and applications. The interconnection of these embedded devices is relied upon to client in mechanization in almost all fields, while likewise empowering advanced applications like a smart grid and extending to regions, for example, smart cities [. Next generation IoT applications must be able to capture, collect, interpret, and act on vast amounts of information which detect the connectivity gaps, handling interruptions, and meeting specific business and industry requirements. An IoT platform makes it possible to develop, deploy, and manage IoT and M2M applications. Automate processes and network connections, stores and manage sensor data, connect and control your devices, and analyse your data. As companies collect data beyond traditional IT boundaries, IoT security measures will be critical. Some key considerations include being able to secure and monitor devices, encrypt sensitive data, and build risk mitigation into systems. IoT data management technologies ensure that you can collect the right data at the right time, even when connectivity is interrupted. Rely on in-memory systems to process massive data volumes generated by thousands of devices.

Fig. 1. Representation of IoT[7]

Main Characteristics of Internet of Things are: Intelligence, Connectivity, Dynamic Nature, Enormous scale, Sensing, Heterogeneity, Security. In this project we focus on Security issues. NODEMCU is an open source IoT platform .It includes firmware which runs on the ESP8266 Wi-Fi and hardware which is based on the ESP-12 module. It can act as both access point and general users. It is very useful in the places where don't have internet. NODEMCU can communicate with in the range of 1000 meters and using NODEMCUs the communication can be easily done within the region. The main advantage of the NODEMCU is it can act as both client and server and it is of less cost so we can use it very easily. Suppose many NODEMCUs are present in a region to send the data from first one to the last one, the data while receiving it acts as a server and while sending it acts as a client.

A. Security Issues in IoT

The dominant part of security attacks will happen at the software level since it is as of now most mainstream and can at the same time cover multiple devices in the network. One of the Security issue is Botnet. Botnets have an extensive variety of atrocious purposes including email spam conveyance, appropriated distributed denial of service(DDoS) attacks, secret key breaking using brute force attack, key logging, and cryptographic moneymining .Bots can consequently check whole system goes and spread themselves utilizing known vulnerabilities and week passwords on different machines. Once a machine is compramised, a little program is introduced for future initiation by the botmaster, who at a specific time can train the bots in the system to execute activities, for example, sending requests to an objective site with the of rendering it not able to serve asks for by real clients, bringing about DDOS.[2]IoT systems don't have well defined perimeters and continuously change due to device and user mobility. IoT systems are highly heterogeneous with respect to communication medium and protocols, platforms, and devices. IoT devices could be autonomous entities that control other IoT devices. IoT systems might include "things" not designed to be connected to the Internet. IoT systems, or portions of them, could be physically unprotected and/or controlled by different parties. Unlike smartphone applications, which require permission for installation and many user interactions, granular permission requests might not be possible in IoT systems because of the large number of devices.

B. Security Vulnerabilities in IoT Devices

These security issues are reasonable and would provide a first line of defence but their application is clearly limited by the scalability of human interaction with IoT device.

1) *Insecure web, mobile, cloud interface:* Inability to change default usernames and passwords, weak passwords, absence of powerful password recuperation systems, uncovered accreditations, absence of record lockout, susceptibility to crosswebsite scripting, cross webpage for fabrication, and additionally SQL injection.
2) *Insufficient authentication, authorization:* Privilege escalation, lack of granular access control [6].
3) *Insecure network services:* Vulnerability to denial-of service, buffer overflow, and fuzzing attacks; network ports or services unnecessarily exposed to the Internet.
4) *Lack of transport encryption/integrity:* verification Transmission of unencrypted data and credentials.
5) *Privacy concerns:* Collection of unnecessary user data, exposed personal data, insufficient controls on who has access to user data, sensitive data not de-identified or anonymized, lack of data retention limits.
6) *Insufficient security configurability:*Lack of granular permissions model, inability to separate administrators from users,weak password policies, no security logging, lack of data encryption options, no user notification of security events.
7) *Insecure software/firmware*:Lack of secure update mechanism, update files not encrypted, update files not verified before upload, insecure update server, hardcoded credentials.
8) *Poor physical security:* Device easy to disassemble, access to software via USB ports, removable storage media [4].

II. PROPOSED METHODOLOGY

The most notable practical use of prime numbers is in cryptography. Many popular algorithms used in public-key cryptography, which has numerous and extremely important security applications are based on the fact that integer factorization is a "very hard" problem. What this means is that the time required to factorize integers into their prime factors grows exponentially with the number of bits in the integer. So if the encryption uses very large integers, it would take an unrealistic amount of time to crack it [4]. In formal number theory a Gödel numbering is a function which assigns to each symbol and formula of some formal language a unique natural number called a Gödel number (GN). The concept was first used by Kurt Gödel for the proof of his incompleteness theorem. Gödel used a system based on prime factorization. He fist assigned a unique natural number to each basic symbol in the

formal language of arithmetic with which he was dealing [3].To encode an entire formula, which is a sequence of symbols, Gödel used the following system. Given a sequence

$$(x_1, x_2, x_3, ..., x_n) \quad (1)$$

of positive integers, the Gödel encoding of the sequence is the product of the first n primes raised to their corresponding values in the sequence:

$$\text{enc}(x_1, x_2, x_3, ..., x_n) = 2^{x1} .3^{x2} .5^{x3} ...p^{xn} \quad (2)$$

According to the fundamental theorem of arithmetic, any number can be uniquely factored into prime factors, so it is possible to recover the original sequence from its Gödel number.

Figure 3 depicts the flowchart of the algorithm of this process. Take the Input from User through keypad and Apply Gödelization for given Input, Check for Password if it correct password it allow to system for Access Point if it is Wrong Password it agains asks for correct password. In this first step is taken the input data from the user. Here we are using a NODEMCU IoT device to check for password protection. The IoT device collects the information and applies gödelization formulas to it. In gödelization process, the division of the each digit of the given password and apply the formula (2). Then compare with already existing secret data in code. After checking Integrity of password it gives information to the controller. If it is correct password, then allows the controller to set up the configuration for Access Point (AP). The NODEMCU acts as a access point and after the server gets started then it acts as a hotspot and then it checks all the clients which are to be connected. The integrity of the password fails, and then NODEMCU will not provide access points to any other clients. I asks for correct password toa user who works with server NODEMCU.

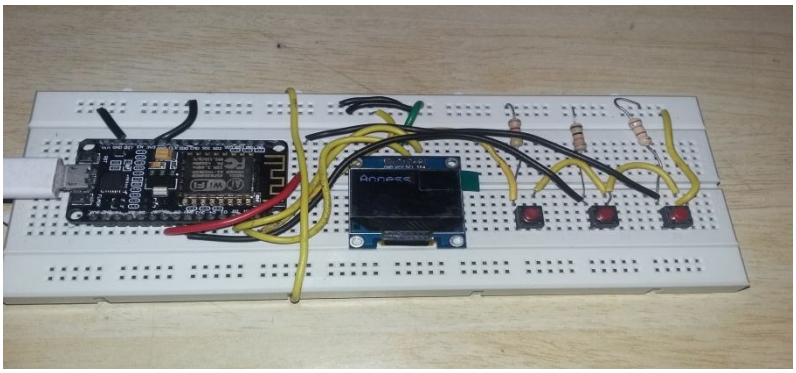


Fig 2. NODEMCU & OLED KIT used for Gödelization

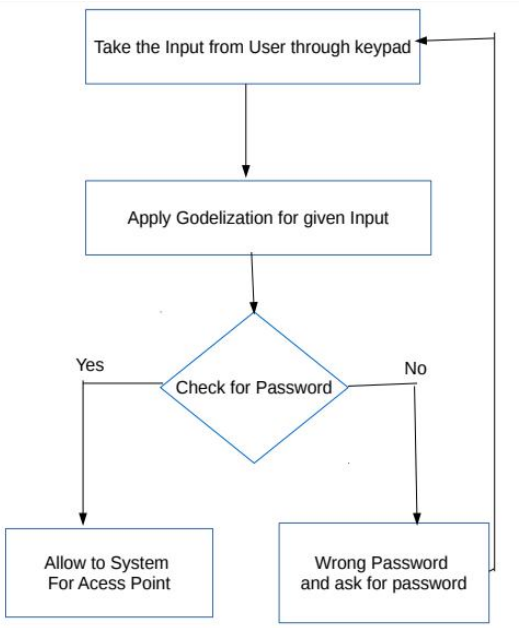


Fig. 3 Flowchart for an algorithm

A. Godel Number Sequence

A mathematical concept termed asgödelization is used as an encoding scheme. The scheme of gödelization is explained as prime factorization theorm. It states that every positive integer greater than one can be factored into multiplication of primes, and this factorization is unique except for difference in the order of the factors. To factor a number 'n' is to write it as product of other prime numbers.

N=a*b*c

Factoring a number is relatively hard compared to multiplying the factors together to generate the number. For any number 'n' of natural numbers, the godel number sequence(GNS) is given by:

GNS(n)=(x0,x1,x,……xk)where n=(2^x0)*(3^x1)*(5^x2).……((PrNo(k) is the k thprimeExample:90=2^1*3^2*5^1

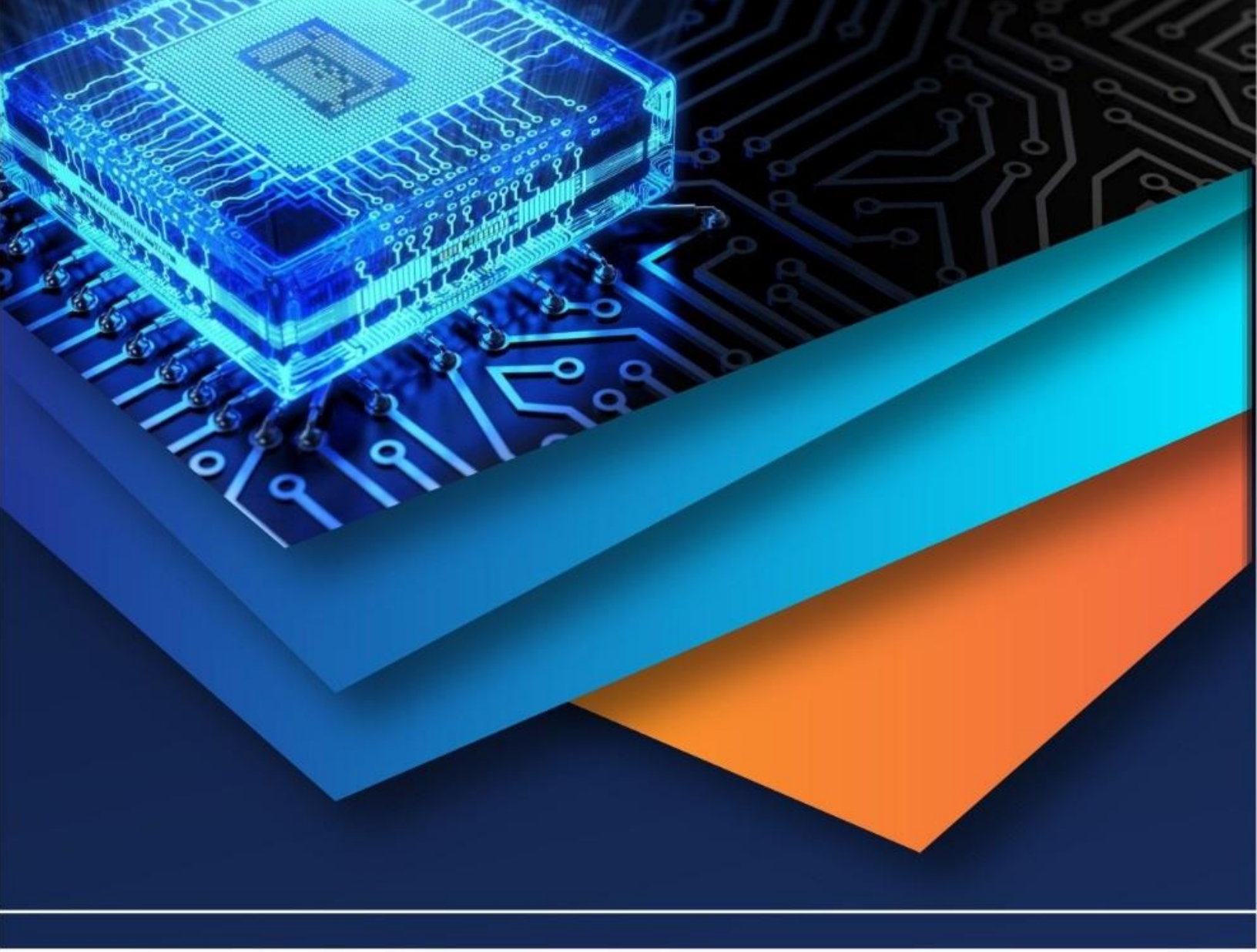
GNS(90)=(1,2,1)

III.CONCLUSION & FUTURE WORK

Now a days drastic growth of IoT devices for communications. They can communicate without any INTERNET provided by anyone. They itself creates wifi communications for transferring the data between devices in the network. The IoT will associate billions of devices to the Internet and reclassify the economic entities, and government associations which will cooperate with the physical world. As per security aspect this project gives a small solution for password protection. The Gödelization is completely used prime factorization to detect the password in the code. Hard to identify the password because of the prime factorization method. This Gödelization method can extend to communicate with the clients. The same Wifi network has multiple clients, they can communicate the data securely. Many secure passwords can use for different transmissions of data in between clients.

REFERENCES

[1] CharithPerera,Chi Harold Liu, SrimalJayawardena, Min Chen A Survey on Internet of Things From Industrial Market Perspective, 3rd ed. IEEE Access, Pages 1660 - 1679,2014
[2] TengXu , James and MiodragPotakonjak, Security of IoT systems: design challenges and opportunities. IEEE/ACM International Conference on Computer-Aided Design ,Pages 417-423 ,2014.
[3] D LalithaBhaskari, PS Avadhani, A Damodaram ,A Combinatorial Approach for Information Hiding Using Steganography And Gdelization Techniques Journal of IJSCI, Pages 21-24,2007
[4] P.Rajamani,DLalithaBhaskari ,A Secured Approach for Watermark Embedding using Key based Gdelization Technique under Spatial and Frequency Domains. International Journal of Computer Applications ,Volume 95 - Number 19,2014
[5] Elisa Bertino,NayeemIslam,Botnets and Internet of Things Security. Computer Published by the IEEE Computer Sciety,2017
[6] H. Sundmaeker, P. Guillemin, P. Friess, and S. Woelffl, Vision and challenges for realising the Internet of Things European Commission Information Society and Media,2010.
[7] https://en.wikipedia.org/wiki/Internet_of_things



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY