e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:04/April-2022 Impact Factor- 6.752 www.irjmets.com

CYBER SECURE AUTONOMOUS CONTROLLED ROBOTIC CAR

Muhammad Shams Ul Arifeen*1, Basit Ali*2

*1,2Department Of Computer Systems Engineering (CSE), UET Peshawar, Pakistan.

ABSTRACT

The human waiter often creates problems in restaurants, hotels and offices. They make mistakes with customer's orders. Most of the time, waiters forget to make a change or add a precise item and also forget to place the customer's order to the kitchen. In addition, the customers also have to wait for the waiters to give their orders. The waiter is the one who remembers the food item and the customer is bound to depend on the waiter where there are so many possibilities of error occurrences. A robot waiter can solve these problems smartly. Therefore, there is a need to design cyber secure autonomous robot to carryout tasks, whereas commands are sent to the waiter robot via communication network. The problem of restaurant automation deals with the design of a communication system and a waiter robot which can coordinate. The security architecture for such robot is extremely complex due to varied resource limits of end nodes and the conspicuous features of a WSN. The future of robot technology can be assured if the security challenges related with it are solved and identified. Our goal is to design a cyber secure framework autonomous controlled robotic car that measures the environmental factors like humidity, temperature, light intensity, and atmospheric pressure and send this information to a server, and use this system as a base to develop a method that is lightweight and ensure the confidentiality of the data in IoT during transmission to the server where data are stored.

Keywords: Autonomous, Cyber Security, Car, Robot.

I. INTRODUCTION

The Internet of Things (IoT) is a network of physical objects, automobiles, household appliances, and other things that are integrated with hardware, sensors, software, and connections, allowing these items to connect, collect and exchange data [1]. The number of IoT devices are growing day by day. The system where appliances are embedded with software, sensors and actuators is known as IoT. The devices are able to transfer data over a network and also communicate with each other. A thing in the IoT can be human having heart monitor insert, can be an injectable ID chip for farm animal, an automobile that has in-built sensors to aware the driver when the pressure is low, a refrigerator with sensors mounted for temperature monitoring or any other natural or manmade object that is provided with unique identifier and is able to transfer data over an internet [2].

Cybercrime is a crime that involves a computer and a networks. It was the 2nd most reported crime in recent years. According to a survey, by 2020, 25 percent of cyber attacks against enterprises will involve IoT devices [3]. So, security of these devices is crucial and is a major concern now a days.

Security and Privacy Issues

IoT connects billions of smart devices to the Internet and their use and applications are spreading day by day. Hence, nowadays it is the topic of interest for technologists in the market. It includes the use of billions of nodes, data points and routers servers. The main issue with them is their lack of security, which must all be addressed [4].

One of the most well known recent IoT attacks was Mirai, a botnet that hacked domain name server provider Dyn and brought down several websites for a prolonged period of time in one of the largest distributed denial-of-service (DoS) assaults ever seen [5]. Attackers were able to obtain access to the network by taking advantage of inadequately protected IoT devices. Since IoT devices are so thoroughly linked, a hacker only needs to exploit one vulnerability to corrupt all of the data and render it useless. Manufacturers who fail to update their equipment on a regular basis or at all leave them open to hackers.

Cyber Security

Cyber security is defined as the protection process to defend computers, servers, mobile devices, electronic systems, networks, and data from cyber-attacks. The purpose of these cyber-attacks is accessing or destroying confidential information; stealing money from users; or disturbing normal business processes.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:04/April-2022 Impact Factor- 6.752 www.irjmets.com

Implementation of effective cyber security is particularly challenging today because of the large number of devices than people, and hackers are becoming more smatter and innovative.

Some of the common categories of security are discussed below.

- Network security offers safeguarding a network of computer from hackers.
- Application security protects applications and equipment free from threats.

II. LITERATURE REVIEW

Although a lot of study has been done in the area of cyber security of WSN and IoT but there is still lot more to do. A brief summary of some developments and futures challenges in IoT are compiled in the form of sections. The [6] paper shows research on denial of service in sensor networks. DoS refer to an adversary's attempt to disrupt, subvert, or destroy a network. A DoS attack is any event that diminishes or eliminates a network's capacity to perform its expected function. A DoS can be caused by hardware problems, software defects, resource exhaustion, environmental variables, or any sophisticated interaction of these factors. The paper discuss DOS attacks at various layers of WSN such as jamming and tempering at physical layer, collision at link layer, homing, neglect and greed misdirection, black holes, monitoring, authorization and redundancy at network and routing layer. Flooding and desynchronization at transport layer. The paper proposes two improvements that can minimize the threat of DoS threats. Alec Woo and David Culler describe a series of improvements to standard MAC protocols called adaptive rate control and the second one is Chenyang Lu's real-time location-based protocols (RAP) provide a real-time communication architecture integrating a query-event service API and geographical progressing with a hybrid displacement monotonic scheduling policy.

The paper [7] published in the 7th International Conference of IEEE on Oriented service Computing and Applications held in 2014 under the name of "IoT based Security: Ongoing issues and Research Opportunities" discusses the ongoing issues and research opportunities on IoT. Object identification and locating, authentication and authorization, privacy light weight cryptosystems and security protocols, software vulnerability and malwares are the challenges that IoT face nowadays. Another paper published under the name of "IoT based Security: Existing grade, issues and Future Measures" in 10th International Conference for Internet Technology and Secured Transaction (ICITST-2015) discusses security threats at different level of IoT i.e. at prospective layer security can be breached by disturbing the transmission media by jamming , tempering and spoofing signals. The network layer is also susceptible to DoS attacks, eavesdropping and passive monitoring. At transport layer issues like authentication and authorization need to be resolved. The paper [8] provides a deep overview of several important features of AES algorithm in details and shows evolutionary history of some previous researches and modifications that have been done on it also comparing it with other algorithms such as DES, 3DES, Blowfish. One of the most extensively used symmetric block cypher algorithms used worldwide is the Advanced Encryption Standard (AES). The algorithm follow a particular structure in repetitive steps to encrypts and decrypts sensitive information and it is used in hardware and software all around the world. It is tremendously tough to crack the cypher encrypted by AES algorithm and get the real information. No evidence has been found till date of cracking this algorithm. AES has three different key sizes such as AES 128, 192 and 256 bit and each of this ciphers has 128 bit block size. But the short comings of the cipher are that means that it performs calculations on blocks of data.

In [9], the main feature of a public-key cryptosystem is that it uses two different keys for encryption and decryption: a public key and a private key. Because the private key cannot be inferred from the public key, it allows the encryption key to be published without exposing the secrets. Until now, RSA is known as the most significant public key cryptography algorithm, it can resist almost all the known passwords attacks so far. It can not only be used for encryption, but also can be used for authentication. When compared with Hash signature, in public key algorithms, the disadvantages include; The RSA technique has a number of drawbacks, including the fact that it can be extremely slow in situations when vast amounts of data must be encrypted by the same computer. It requires a third party to check the reliability of shared public keys. In cryptography, key exchange is the process of exchanging cryptographic keys for encryption between sender and receiver, with such keys being utilised in cryptographic algorithms such as AES. In [10], it is suggested that the sender and reciever can exchange messages encrypted by such keys. The secure technique of exchanging secret keys is provided by public key cryptography. By using key exchange methods both gatherings can exchange the keys or data in a

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:04/April-2022 Impact Factor- 6.752 www.irjmets.com

communication channel so that only the sender and recipient have access to it can understand those. This paper presents Diffie-Hellman key exchange method, which is one of the first public key cryptographic protocols used to exchange and build up secret keys between two parties over a frail channel. Diffie-Hellman is a mathematical algorithm that allows two PCs to use the publicly shared key and produce an identical shared secret on both systems, despite the fact that those systems might never have communicated with one another.

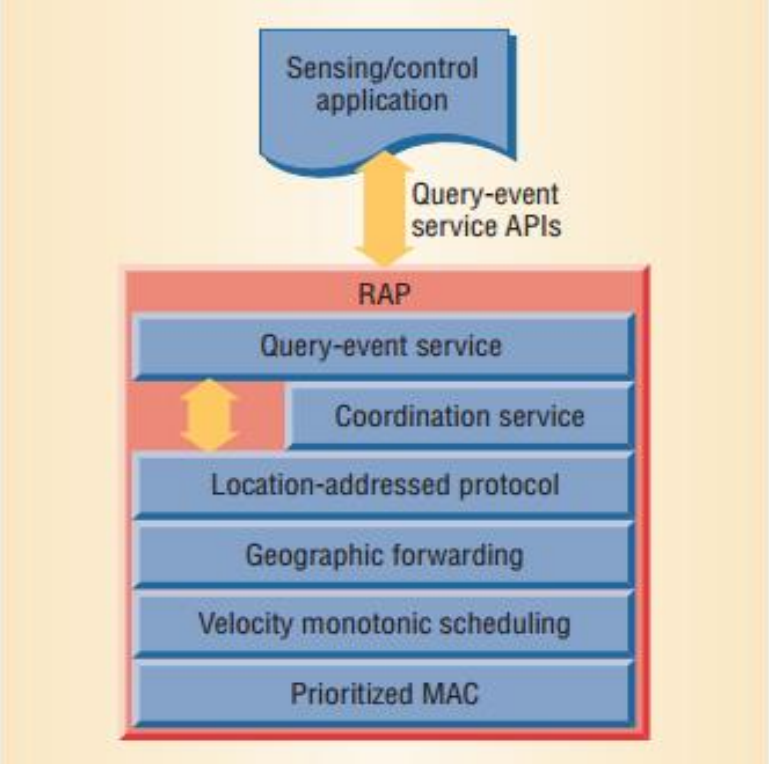

Figure 1: Real-time location-based protocols architecture

III. METHODOLOGY

The proposed method includes the use of Arduino Microcontroller and BLE supported device communication. The entire idea is to build an application for Smart phones which store the order data locally and transmit it to server also. Now the furthermost significant thing is to secure the entire communication. For this persistence, we use OTP security algorithm.

The main steps involved in this paper are:

- To develop an Autonomous Controlled Robotic Car
- To secure the transmission of data by encryption techniques
- To prevent unauthorized person to access the system

Required Tools

A brief explanation of the required hardware and software tool along with usage guidelines is provided in this section.

- Arduino Microcontroller
- Arduino IDE
- Code Composer Studio

Setting Up Development Environment

1. Download Code Composer Studio setup file
2. Run CC studio, select CCs App Center
3. Click and run Resource Explorer in the Code Composer Studio Menue
4. Download BLE stack
5. Import example project from BLE

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:04/April-2022 Impact Factor- 6.752 www.irjmets.com

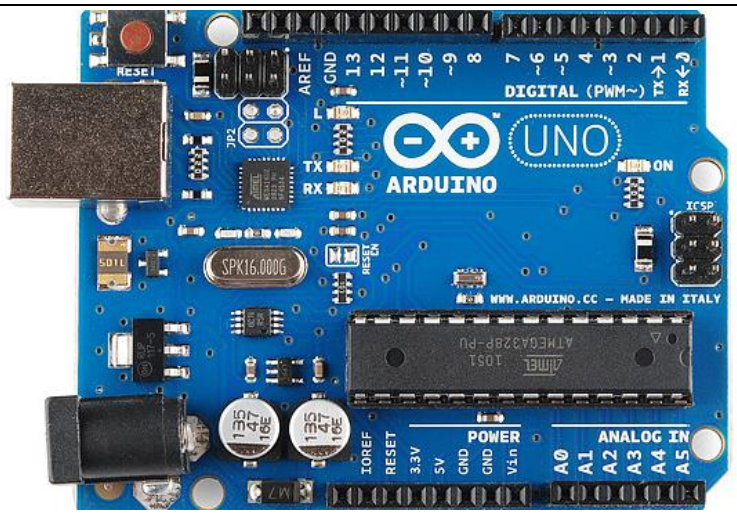

Figure 2: Arduino microcontroller

IV. RESULTS AND DISCUSSION

The system which captures the environment or reads the surroundings, collecting and recording data through sensors. Our monitoring system monitors following parameters of the surroundings.

Taking order from different table

You can watch real time information collected by the system on your IOS and Android mobile devices through App. You can send your data on cloud and it can be accessible from anywhere.

To retrieve data from the Arduino we used console.

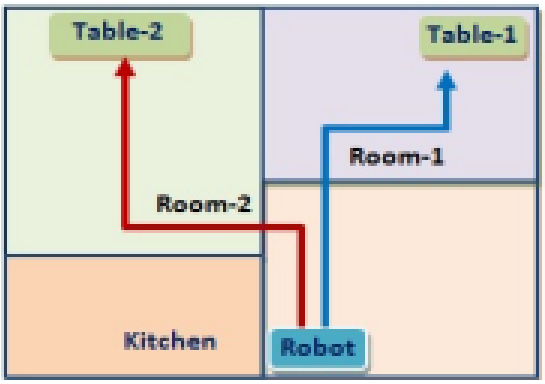

Figure 3: Layout of autonomous controlled robotic car

One Time Pad Security Algorithm

One-Time Pad (OTP) is an encryption technique in which a private key is generated randomly and combined (XOR) with the plaintext to encrypt the message. OTP is a type of Vigenere Cipher. It was developed by banker Frank Miller in 1882 then it was re-invented by Gilbert Vernam and Joseph Mauborgne in 1917. When applied correctly, the OTP provides a truly unbreakable cipher.

An example explains the working of OTP:

Pre-shared Random Bits = 10100100101010101110100100001010111101010011101000 11

Plain text = 110101010101010010100

Length (Plain Text) = 21

Lenght Key (21) = **101001001010101011101**

Encryption:

Key (21) = 101001001010101011101

Plaintext = 110101010101010010100

Bitwise XOR

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:04/April-2022 Impact Factor- 6.752 www.irjmets.com

cyphertext = 01110001111111001001

Decryption:

Preshared Random Bits = 10100100101010111010010000101011110101001110100011

cyphertext = 01110001111111001001

bitwise XOR

Plain text = **11010101010100100100**

V. CONCLUSION

For past few decades, research has been carried out on the connectivity of physical objects to the Internet so that objects can be monitored and controlled from anywhere any time. That revolutionary wave is called Internet-of-Things (IoT). Our architecture provides a base model for secure energy management system. The proposed prototype is tested successfully. Furthermore, this architecture can be extended to secure monitoring of silos and in the agriculture fields.

So the primary objectives of our paper were: firstly, unauthorized person can connect with the system but it will get encrypted data; secondly, we can analyze the power consumption of the sensors as they uses coin cell battery to power which needs to be changed after few weeks.

VI. REFERENCES

[1] K. Ashton, "That 'Internet of Things' Thing," RFID Journal, [Online]. Available: https://www.rfidjournal.com/articles/view?4986.

[2] D. Evans, "The Internet of Things How the Next Evolution of the Internet Is Changing Everything," [Online]. Available: https://www.supplychain247.com/paper/the_internet_of_things_how_the_next_evolution_of_the_internet_is_changing/Internet_of_Things.

[3] Cybercrime Damages, "Cybercrime Damages," CYBERCRIME MAGAZINE, 2016. [Online]. Available: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016.

[4] J. Manyika and M. Chui, "By 2025, Internet of things applications could have $11 trillion impact," Fortune, 2015.

[5] NCCIC, "Understanding Denial-of-Service Attacks," CISA. [Online]. Available: https://www.us-cert.gov/ncas/tips/ST04-015

[6] A. Wood and J. Stankovic, "Denial of Service in Sensor Networks," IEEE, vol. 35, no. 10, p. 9, 2002.

[7] Z. Zhang and M. Yi Cho, "IoT Security: Ongoing Challenges and Reasearch Oppurtunities," in IEEE, 2014.

[8] M. Abdullah, "AES Algorithm to Encrypt and Decrypt Data," p. 13, 2017.

[9] X. Zhou and X. Tang, "Research and Implementation of RSA algorithm for Encryption and Decryption," p. 4, 2011.

[10] S. Kallam, "Diffie Helmen: Key Exchange and Public Key Crypto Systems," p. 27, 2015.