Securing Data Transmission Using DES For Smart Home Monitoring System

P.Vedavalli, K.Krishnaveni, J.K.R.Sastry

Abstract: In the modern age and digital era the data security is increasing demand. Most of the researchers and scientists around the world are discovering measures to provide data security for data transmission without any loss of data or theft of data. The whole of cryptography deals with the methods and algorithms used for the data transmission without causing any attacks on them. Her using a 56-bit keyword and 64-bit message to transmit the data from the transmitter to the receiver. In this project, the controller will take care about transmission of various devices data. The devices data should be encrypted and that data should be stored in the cloud .56-bit key is generated along with 64-bit message that will be decrypted by the authorised person

In this paper, the technique for secure data transmission while maintaining the authenticity and integrity of the message. The data encryption at the transmitter and the data decryption at the receiver is done successfully and the plaintext is retrieved without any errors.

Index Terms: IoT, Encryption, Decryption, and Cryptography.

I. INTRODUCTION

The early years of the Internet-of-Things (IoT) primarily involved electronic communication through machine to machine interactions. However, the idea has evolved rapidly to incorporate human interactions moreover, ushering in associate degree era of Internet-of-Everything. Today, our world includes billions of sensors and computing devices that are regularly sensing, collecting, consolidating, and analyzing the vital quantity of our personal info. Such info might embody our location, contact list, browsing patterns, and health and fitness information.[9] The sensing, collecting, and propagating of such intimate personal knowledge by computing devices are primarily motivated by convenience: as devices get smarter, they'll react better to our wants, wishes, and even and handle emergencies sadly, this convenience comes at the expense of security and privacy challenges: the non-public, personalized info, if accessible to associate degree unauthorized, malicious agent, may end up in vital damage to our wealth, reputation, and private security. In addition to our own[8] personal information, these devices additionally embody assets introduced by their makers at numerous stages during their production offer chain. These embody fuses, firmware, and rectify modes. Unauthorized access to those assets may end up in the loss of lots of greenbacks in taken intellectual properties, in addition as doubtless dangerous misuse of the assets. With the ever-present preparation of these devices, such security vulnerabilities may be catastrophic.

Now a days every device should acts like an smart. Every device in the home is acts like a smart with the help of wireless communication protocols Zigbee, WiFi, Bluetooth, IR, etc.The devices which is connected to the network should be monitoring and management of appliances of the systems which are lightining and heating.

The point of computing devices having such doubtless catastrophic vulnerabilities isn't just tutorial. It can happen unfortunately too simply in follow. There have been varied demonstrations of attackers being easily ready to inject malicious code directly into wearable devices by victimization programming interface and so acquire sensitive information of users [2]. There are incontestable attacks on implantable medical devices, like implantable cardioverter electronic device[3], that seriously threaten the patient's life safety. Attacks in business and concrete infrastructure additionally show an increasing trend. within the field of automotive embedded systems, a lot of and more electronic devices and embedded devices are employed in several high-end automobiles.

The offender will gain management of the automotive due to the dearth of security protection in these devices, such as electronic management unit attack [4]. This is able to have a serious security threat to the motive force. Attacks on urban infrastructure will have an effect on the social order, like attacks on transportation and supply.

Cryptography is Associate in Nursing art of security technique wherever messages are encoded in a very non-readable kind. In easy words, it's nothing however a way utilized in the protection of information throughout the transmission from sender to receiver and unauthorized access is denied. Therefore, security and confidentiality is incredibly a lot of needed during this side. the main target and discussion during this paper would get on varied techniques of encryption and decryption. The Cryptographic primitives are exacting in terms of computation resources: public key cryptography needs dearly exponentiations; centrosymmetric ciphers use multiple iterations of lexicon lookups and permutations that are consecutive ordered; secure hashes repeat repetitive rounds of shifts and permutations.

Revised Manuscript Received on May 10, 2019.

P.Vedavalli, Department of ECM Koneru Lakshmaih Educational Foundation, Vaddeswaram,Guntur Dt

K.Krishnaveni, Department of ECM Koneru Lakshmaih Educational Foundation, Vaddeswaram,Guntur Dt.

Dr.J.K.R.Sastry, Department of ECM Koneru Lakshmaih Educational Foundation, Vaddeswaram,Guntur Dt

With a lot of client applications requiring cryptanalytic operations in their algorithms for security and privacy, hardware makers propose hardware implementations of those widespread primitives. the benefits of exploitation hardware are lower latency for operations, higher output for prime volume transactions, and lower overall power consumption.[10] Like most hardware implementations, the value is higher complexness and value of the hardware, and flexibility, as the semiconductor area is reserved for the mounted operations. as a result of hardware style problems are thought[7] of once cryptanalytic standards are chosen, educational and business implementations of cryptanalytic protocols are essential.

II. RELATED WORK

To enhance the protection of information transmission in Bluetooth communication, a hybrid coding algorithmic program supported DES and RSA is projected. The presently used coding algorithmic program utilized by the Bluetooth to guard the confidentiality of information throughout transport between 2 or additional devices could be a128-bit bilaterally symmetrical stream cipher known as E0. it should be broken underneath sure conditions with the time quality O(264). Within the projected hybrid coding algorithmic program, rather than the E0 coding, DES algorithmic program is employed for knowledge transmission owing to its higher potency in block coding, and RSA algorithmic program is employed for the coding of the key of the DES owing to its management blessings in key cipher. Underneath the twin protection with the DES algorithmic program and also the RSA algorithmic program, the info transmission within the Bluetooth system is safer. Meanwhile, it's clear that the procedure of the complete coding continues to be straightforward and economical as ever. Additionally, the confidentiality of the hybrid coding algorithmic program is additionally mentioned.[1].

With the appearance of low price Field Programmable Gate Arrays (FPGA's), building special purpose hardware for computationally intensive applications has currently become attainable. The cryptography of block ciphers involves huge computations that area unit freelance of every alternative and may be instantiated at the same time so the answer area is explored at a quicker rate. This paper presents the planning for Hardware implementation of knowledge encoding customary (DES) cryptography on FPGA victimization complete key search. 2 architectures viz. reiterative and Loop unrolled DES design area unit enforced.[2].

Encryption may be a very important method to make sure the confidentiality of the knowledge transmitted over the insecure wireless channel. However, the character of the wireless channel tends to deteriorate due to noise, interference, and weakening. Therefore, the encrypted transmitted signal is going to be received with some quantity of error. Consequently, because of the strict avalanche criterion (SAC), this error propagates throughout the cryptography method, leading to 0.5 the bits (on average) when cryptography to be in error. So as to alleviate this quantity of error, sensible cryptography techniques and/or new coding algorithms that take into consideration the character of wireless channels are needed. On the opposite hand, these solutions would possibly degrade the protection of the knowledge and therefore the turnout of the wireless channel. During this paper, we tend to propose a brand new coding algorithmic program that uses associate optimized framework for the turnout and security.[3]

To subsume the threat of power analysis to secret writing device, a replacement power analysis resistant DES algorithmic rule design is projected, that is combined with “asymmetric” mask technique. And its digital hardware circuit is intended. Then its power analysis attack resistant ability is tested. Compared with non-protected DES, victimization nearly five times larger samples and attack time, the key of the projected DES still cannot be gained through correlation power analysis. Experiment results show that the designed DES algorithmic rule incorporates abound opposed power analysis result.[4]

In this age of explosive growth in info exchanges, there's so no time at that security doesn't matter. One among the radially symmetrical encoding algorithms, DES, has unbroken its dominant position within the space of information encoding over a previous couple of decades. However, with a fast development within the field of hardware, DES has already been tested insecure. It takes a brief time to translate the ciphertext to its corresponding plaintext mistreatment brute-force technique at an inexpensive price. This is often chiefly because of the tiny key size DES used. Given these problems, the target of this text is to counsel an alternate on DES to get higher security and higher execution potency by increasing the key size and change the iteration technique. Comparisons were conducted with each DES and also the advanced DES named triple DES (3DES). The results have incontestable that the planned algorithmic program outperforms each previous algorithms.[5]

Various sectors like the retail, welcome, banking and monetary introduced data technology years back. Current enhancements have perpetually offered a wider scope of growth to those sectors. Zooming within the Banking sector most banks are currently providing web banking services. The objectives of introducing the e-banking services were profits, quick service, improved productivity, client satisfaction, 24x7 operations savings. The maximum amount the expansion of net probes the purchasers to use the new online services & banks to supply the same; equally it makes the purchasers & business skeptical concerning the protection being enforced. The business must make sure the security of every electronic dealing over the web. Vital areas to focus for this area secure communicating, the third party for info maintenance non-breach able encoding technique. Any on-line dealing constitutes confidential information. Any injury there to information or hacking of that information could bring a vital quantity of loss to each the parties concerned. Cryptography could be a widely used science for secret writing. Coding is one method of secret writing.

The method involves a key associated a formula to get a Ciphertext (secret code) from an understandable text. On the opposite hand, coding helps to retrieve the initial text exploitation constant key. Currently, what's the key here? The secret's the core string (word) being employed within the formula. it's unbroken personal. Cryptography has classified the keys being employed within the method as key algorithms are most ordinarily used kind wherever one secret's used for each coding and coding. In uneven key algorithms, completely different keys are used each for coding and coding.[6]

III. PROPOSED MODEL

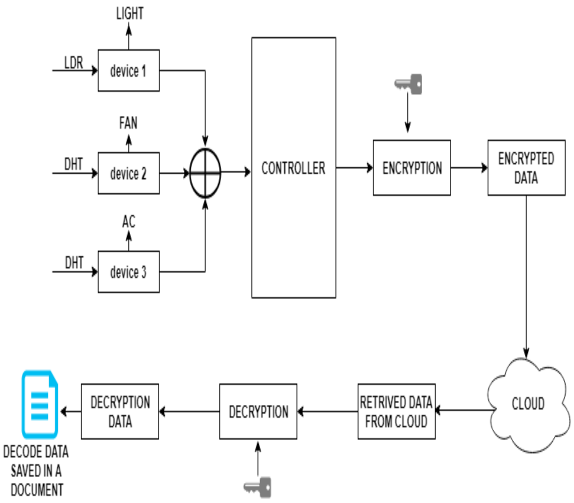


Fig.1: Proposed Model

Here the data is captured from the various sensors. Those data are controlled by the controller To recognize that the manner the information security and privacy have become a burning issue and to produce the data security and privacy has been a various state of affairs.

To keep up the information security and privacy the cryptography system have a range of algorithms that successively helped the users to send the data employing a reliable technique. One among the foremost widespread encryption rule we have a tendency to utilize in this paper is that the encoding normal. This rule provides the users the flexibleness to use a 56-bit length keyword and a 64-bit length message or plaintext.

Though there are several algorithms associated with cryptography that provides additional bit lengths for information and also the keyword, however, the DES is that the straightforward to grasp and implement. It's associate degree uneven key rule that makes use of public and personal. As the name itself the general public key's know to reach the consumer and host, the non-public keys recognize solely to the consumer itself. It's sort of block cipher that divides the plaintext into the blocks and additional cryptography are going to be followed.

Associate degree extension to the DES is that the triple DES rule during which the information cryptography is going to be happening for 3 times or briefly the DES algorithm once-perennial for three times is termed as triple DES of these give just one factor that's the safety and privacy associated with the information.

The advantage with a key length which gives intensive security whereas playing the Brute-Force attack. Virtually it'll take a decade for the attack to induce the key that was used throughout the transmission. the sole disadvantage with this rule is that the keys, although they need to be been sensible in stopping the attacks however there's an opportunity of obtaining the identical key if there is endless word within the sequence. The below diagram can represent the flow during which the DES rule is performed for the given message. Here we've used a 10-bit length key and 8-bit length data/message for the cryptography and decipherment.

IV. RESULTS

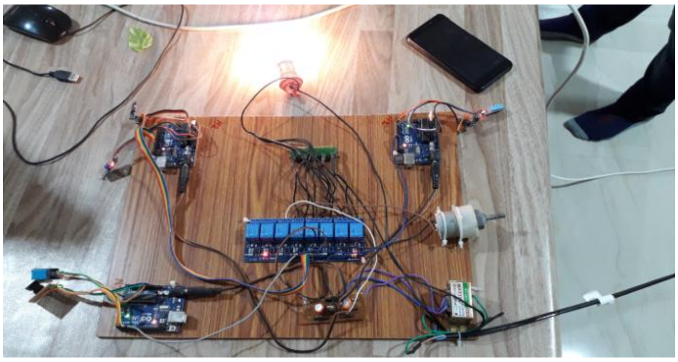
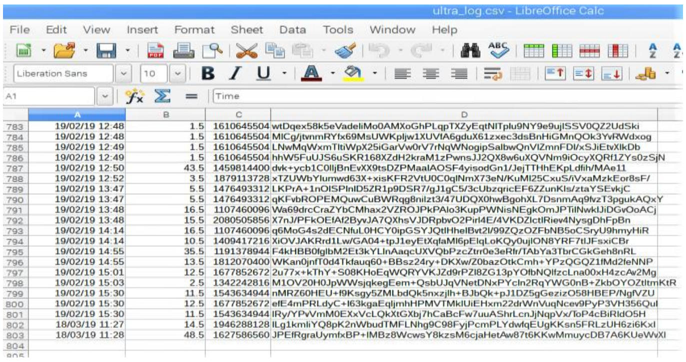


Fig.2: Prototype Model

Every device is connected with Wi-Fi which is taken the sensor data and transmitted to the controller .the home appliances should be controlled automatically switching with the help of relay. In fig.2Based on the environmental conditions the light, fan, AC will be on and off done.

The sensor data is transmitted to the controller with the help of Wi-Fi. Wi-Fi is working with on the basis of MQTT protocol. Sensor data should be transmitted to the controller, it will send the data to encryption and its data will be finally stored into the cloud. At the end of the application, the user will retrieve the data from the cloud and with the help of key the data will be decrypted from the cloud and the data will be accessed by the end user.


ultra_log.csv - LibreOffice Calc
File Edit View Insert Format Sheet Data Tools Window Help
Liberation Sans
10
A1

Time

	A	B	C	D
783	19/02/19 12:48	1.5	1610645504	wtDqex58k5eVadeliMo0AMXoGhPLqpTXZyEqtNITplu9NY9e9ujISSV0QZ2UdSki
784	19/02/19 12:48	1.5	1610645504	MICg/jtvnmRYfx69MsUWKpljw1XUVIA6gduX61zxec3dsBnHiGMnQOk3YvRWdxog
785	19/02/19 12:49	1.5	1610645504	LNwMqWxmTltiWpX25iGarVw0rV7rNqWNogipSalbwQnVIZmnFDI/xSJiEtvXlkDb
786	19/02/19 12:49	1.5	1610645504	hhW5FuUJS6uSKR168XZdH2kraM1zPwnsJJ2QX8w6uXQVNm9iOcyXQRf1ZYs0zSjN
787	19/02/19 12:50	43.5	1459814400	dvk+ycb1C0lljBnEvXX9tsDZPMaalAOSF4yisodGn1/JejTTHhEKpLdfih/MAe11
788	19/02/19 12:52	3.5	1879113728	xTZUWbYlumwd63X+xisKFR2VtU0C0qINmX73eN/KuMI25CxuS/iVxaMzkEor8sF/
789	19/02/19 13:47	5.5	1476493312	LKPrA+1nOISPInID5ZR1p9DSR7/gJ1gC5/3cUbzqricEF6ZZunKls/ztaYSEvkjC
790	19/02/19 13:47	5.5	1476493312	qKFvbROPEMQuwCuBWRqg8nilzt3/47UDQX0hwBgohXL7DsnmAq9fvzT3pgukAQxY
791	19/02/19 13:48	16.5	1107460096	Wa69drcCraZYbCMhax2VZROJPkPAlo3KupPWNisNEgkOmJPTilNwklJiDGvOoACj
792	19/02/19 13:48	15.5	2080505856	X7nJ/PFkOEfAf2ByvJA7QXhsVJDRpbvO2Pirl4E/4VKDZlctlRiev4NysgDhFpBn
793	19/02/19 14:14	16.5	1107460096	q6MoG4s2dECNfuL0HCY0ipGSYJQtlHhelBvt2l/99ZQzOZFbNB5oCSryU9hmyHiR
794	19/02/19 14:14	10.5	1409417216	XiOVJAKRrd1Lw/GA04+tpJ1eyEtXqfaMl6pElqLoKQy0ujlON8YRF7tlJFsxiCBr
795	19/02/19 14:55	35.5	1191378944	F4kHBB0fglbM2Et3kYLInAaqcUXVQbPzcZtrr0e3eRfr/TAbYa3TbrCGkGeh8nRL
796	19/02/19 14:55	13.5	1812070400	WKan0jnfT0d4Tkfauq60+BBsz24ry+DKXw/Z0bazOtkCmh+YPzQGQZ1fMd2feNNP
797	19/02/19 15:01	12.5	1677852672	2u77x+kThY+S08KHoEqWQRYVKJZd9rPZI8ZG13pYOfbNQlfzcLna00xH4zcAv2Mg
798	19/02/19 15:03	2.5	1342242816	M1OV20H0JpWWsjqkegEem+QsbUJqVNetDNxPYcln2RqYWG0nB+ZkbOYOZtltmKtR
799	19/02/19 15:30	11.5	1543634944	nMRZ60HEU+f9Ksgy5ZMLbdQk5nxzjlh+BJbQk+pJ1DZ5gGezizO58HBEP/NgfVZU
800	19/02/19 15:30	12.5	1677852672	efE4mPRLdyC+I63kgaEqljmhHPMVTMklUiEHxm22drWnVuqNcev9PyP3VH356Qul
801	19/02/19 15:30	11.5	1543634944	lRy/YPvVmM0EXxVcLQkXtGXbj7hCaBcFw7uuAShrLcnJjNqpVx/ToP4cBiRldO5H
802	18/03/19 11:27	14.5	1946288128	lLg1kmliYQ8pK2nWbudTMFLNhg9C98FyjPcmPLYdwfqEUgKKsn5FRLzUH6zi6Kxl
803	18/03/19 11:28	48.5	1627586560	JPEfRgraUymfxBP+IMBz8WcwsY8kzsM6cjaHetAw87t6KKwMmuycDB7A6KUeWvXl
804				
805				

Fig.3: Encrypted Data

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

The encrypted should be given as fig3 encrypted data should be sent to the cloud.

V CONCLUSION

The data transmission is successful without any data loss and hence the privacy and security are maintained using the DES algorithm. The data usage will be less, the project can be further extended to the various lightweight algorithms. Moreover, the DES algorithm uses a single key for both encryption and decryption. Lightweight cryptographic algorithms should be implemented in further extension.

REFERENCES

1. Harshali D. Zodpe, Prakash W.Wani,” Design and Implementation of Algorithm for DES Cryptanalysis” 2012 IEEE.
2. Mrs. Mukta Sharma#, Dr. R B Garg, Professor*, Ms. Surbhi Dwivedi, “Comparative Analysis of NPN Algorithm & DES Algorithm”, 2014 IEEE
3. Luminiţa Scripcariu1, Petre-Daniel Mătăsaru1, Felix Diaconu1, “Extended DES Algorithm to Galois Fields”, 2017 IEEE
4. Wuling Ren, Zhiqian Miao “A Hybrid Encryption Algorithm Based on DES and RSA in Bluetooth Communication “2010 IEEE
5. Walid Y. Zibideh and Mustafa M. Matalgah, “ An Optimized Encryption Framework based on the Modified-DES Algorithm: A Trade-Off between Security and Throughput in Wireless Channels” 2012 IEEE
6. ZhouYingbing, LI Yongzhen, “The Design and Implementation of a Symmetric Encryption Algorithm Based on DES” 2014 IEEE
7. Iqra Hussain1, Mukesh Chandra Negi2, Nitin Pandey3” A Secure IoT-Based Power Plant Control using RSA and DES Encryption Techniques in Data Link Layer” 2017 IEEE
8. Li Jie, Lv Yuxiang, Sun Huafang, Shan Weiwei (Corresponding author), “A Power Analysis Resistant DES Cryptographic Algorithm and its Hardware Design”2012 IEEE
9. @Availablehttps://ccm.net/contents/134-introduction-to-encryption-with-des
10. 10.@Available https://www.iusmentis.com/technology

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication