IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2320-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 9, Issue 9, September 2020

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.512

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 9, September 2020||

Modified S-Box in AES Algorithm for Secure Internet of Things Applications

Praveen Singh Patel[1], Prof. Prabhat Sharma[2]

M.Tech Scholar, Dept. of ECE., Oriental Institute of Science and Technology, Bhopal, India[1]

Assistant Professor, Dept. of ECE., Oriental Institute of Science and Technology, Bhopal, India[2]

ABSTRACT: Data communication security for internet of things application will become major issue in 5G communication. Multimedia data security is achieved by methods of cryptography, which deals with encryption of data. Most of the application uses Advanced Encryption Standard (AES) and modify it, to reduce the calculation of algorithm and for improving the encryption performance. In modified AES algorithm used 1-Dimensionla S-box instead of 2-Dimensional S-box. Theoretical analysis and experimental results prove that this technique provides high speed as well as low latency on data encryption and decryption. Modified-AES algorithm is a fast lightweight encryption algorithm for security of multimedia data. All above advantages make algorithm highly suitable for the input message transfer.

KEYWORDS: Wireless, Security, Cryptography, Encryption, Decryption, Block Cipher, Simulation, Xilinx.

I. INTRODUCTION

The Advanced Encryption Standard (AES) has been recently acknowledged as the symmetric cryptography standard for private information transmission. Nonetheless, the normal and malevolent infused shortcomings diminish its unwavering quality and may cause classified data spillage. In this paper, we study simultaneous flaw identification plans for arriving at a solid AES engineering. Cryptography is the study of mystery codes, empowering the secrecy of correspondence through a shaky channel. It ensures against unapproved parties by avoiding unapproved adjustment of utilization. As a rule, it utilizes a cryptographic framework to change a plaintext into a cipher text, utilizing more often than not a key. As systems administration innovation progresses, the hole between system transfer speed and system handling force enlarges. Data security issues add to the requirement for growing elite system handling equipment, especially that for constant preparing of cryptographic calculations.

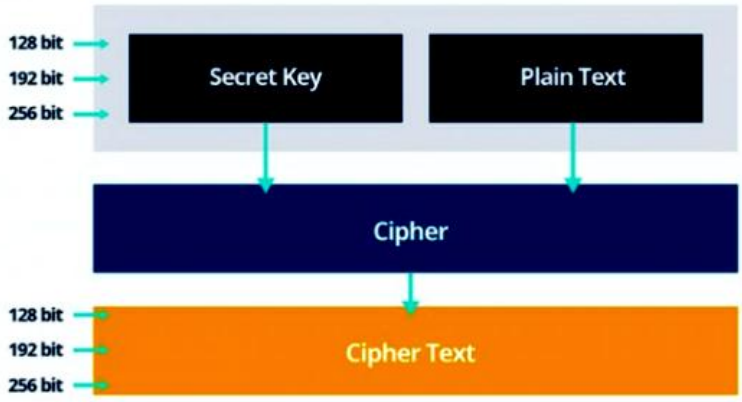

Figure 1: AES Model

AES is fundamentally a security calculation is utilized for encryption and unscrambling of information. Encryption is the procedure where we play out a fixed arrangement of activity on the information to randomize the information and change it into some inane structure so that regardless of whether any unapproved operators gets an entrance of the information, won't almost certainly acquire the valuable data present in the information. Such information which is obviously inane is transmitted. Such information can be changed over back to its valuable structure, that is, the real information just with the key of the key at the less than desirable end. Keys are fundamentally a mystery parallel information of above said fixed length which are utilized to encode (cipher) the first information at the transmitting end to get the scrambled information and decode (de-cipher) the scrambled information to get back the first information at

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 9, September 2020||

the less than desirable end. Clearly the key with the assistance of which the information will be recovered at the less than desirable end will be known at the less than desirable end before the foundation of the correspondence. This procedure of recovering the first information is called unscrambling. The part of science which manages encryption and unscrambling of information is known as Cryptography. The calculations with the assistance of which we actualize encryption or unscrambling of information are called Cryptographic calculations.

II. BACKGROUND

A. R. Chowdhury et al., Internet of things (IoT), internetworking of shrewd gadgets, inserted with sensors, programming, hardware and system availability that empowers to speak with one another to trade and gather information through an indeterminate remote medium. As of late IoT gadgets are overwhelming the world by giving it's adaptable usefulness and constant information correspondence. Aside from adaptable usefulness of IoT gadgets, they are low-battery controlled, little and complex, and experience bunches of difficulties because of risky correspondence medium. In spite of the reality of numerous difficulties, the vitality issue is presently turning into the prime concern. Streamlining of calculations regarding vitality utilization has not been investigated explicitly, fairly the greater part of the calculations center around equipment territory to limit it broadly and to amplify it on security issue as could be expected under the circumstances[1]. A. Priya et al., shows the techniques based on ABE consist of two types: KP-ABE (Key- Policy ABE) where the user's private key is linked to an access structure (or access policy) over attributes and cipher-text is connected to the set of attributes, and CP-ABE (cipher-text policy ABE) is vice versa. Hence, in this, Review we discuss about the various security techniques and relations based on Attributes Based Encryption, especially, the type KP-ABE over data attributes which explains secured methods & its schemes related to time specifications[2].
S. S. Priya, et al., presents a high throughput adjusted Propelled Encryption Standard (AES)- 128 piece calculation is executed. Another expanded parallelism strategy is presented in altered AES engineering in Blend Segment round which builds the general throughput of AES calculation. This method is actualized in XC5VLX50T FPGA gadget Virtex-5. Utilizing this method throughput is expanded 5 % and zone is diminished by 30 % when contrasted with parallel mixcolumn[3]. R. V. Kshirsagar et al., presents high information throughput AES equipment engineering by dividing ten rounds into sub-squares of rehashed AES modules. The squares are isolated by middle of the road supports giving a total ten phases of AES pipeline structure. Furthermore, the AES is inside equitably separated to ten pipeline stages, with the extra component that the move columns square (Move Line) is organized to work before the byte substitute (Byte Substitute) square. This proposed swapping task has no impact on the AES encryption calculation, be that as it may, it streamlines the handling of four squares of information in parallel instead of 16 squares, which is considered as the key preferred standpoint for region sparing. it is have assessed the execution of our usage as far as throughput rate and equipment zone for Xilinx's Simple 3 FPGA. The reproduction results demonstrate that the proposed AES has higher throughput rate of about 4.25% than the general AES pipeline structure with a sparing equipment region of 56%[4].

Abhiram L S et al., presents system security is a rising area of correspondence. Cryptography assumes an imperative job in giving a protected system to correspondence. The most secure square figure today is Rijndael figure otherwise called AES. Yet, with cutting edge investigate occurring in the field of cryptography, the regular plan of AES is powerless for cryptanalysis. Subsequently a great deal of changes has been proposed on this calculation. Static S-Boxes are actualized utilizing look into tables which will never change with the information content or info key. This devours a great deal of Memory for the capacity of look into table. Additionally this strategy makes figuring out extremely straightforward with the end goal of cryptanalysis. Subsequently it is fundamental to produce S-Bytes at run time. It is useful if the S-byte created amid run time shifts with the info key. Another shortcoming of AES is that it works with a solitary key. [5]. M. El Maraghy et al., shows proficient improved territory and speed FPGA execution for the Propelled Encryption Standard is proposed in this work. The iterative circling strategy is received with multistage sub-pipelining engineering to accomplish a 1.33 Gbps throughput for the AES-128 piece Encryption process. The proposed plan works at 425 MHz with 303 CLB cuts on a Xilinx Virtex-5 XC5VLX50 FPGA Gadget. For constant equipment assessment, an end-client Java based application is produced. The product application is connected to the equipment plan through the Xilinx Micro Blaze delicate processor centre[6].

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 9, September 2020||

III. PROPOSED METHODOLOGY

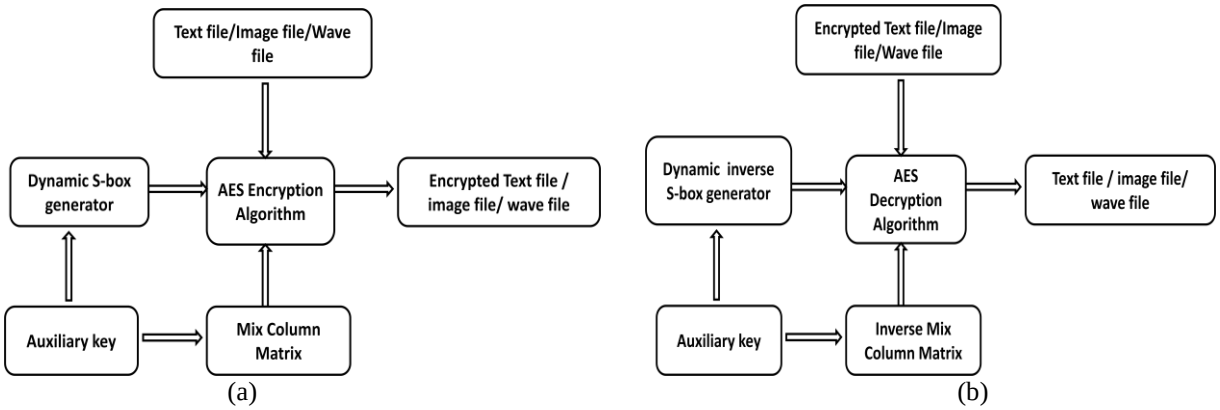

Figure 2: Block diagram of modified AES (a) Encryption (b) Decryption

In Figure 2 show the block diagrams of the new encryption and decryption algorithms to encrypt or to decrypt the text, image or audio files.

The AES algorithm consists of a static S-box and a constant mix column matrix. The possible combinations of secret key to be tried to break the algorithm are 2128 for AES-128 algorithm. Although algebraic attacks like linear and differential cryptanalysis are difficult (they need large amount of plain text and cipher), it has been shown that theoretically it may be possible to break the AES algorithm by XSL attack, by constructing multivariate quadratic equations. Since the S-box is static it is possible to construct these equations. There are nearly 256! _ 21638 S-boxes, if it is generate any one of them, which is a key dependent S-box, it becomes very difficult to attack the AES algorithm. The mix column matrix is a static 4 _ 4 matrix with 16-byte entries, and if it is construct a key dependent mix column matrix then cryptanalysis still becomes more difficult. The necessary condition to be satisfied for this mix column matrix is that it must be a non-singular. These two blocks are explained in the next section. All the remaining operations are the same as in the present AES algorithm.

IV. SIMULATION RESULTS

The designed MAES Security Algorithm implementation has multiple sub-modules inside it both at the Encryption and Decryption end, based on the internal operations of the algorithm. Top module is designed, simulated and synthesized as per proposed algorithm. Now presenting the results of simulation.

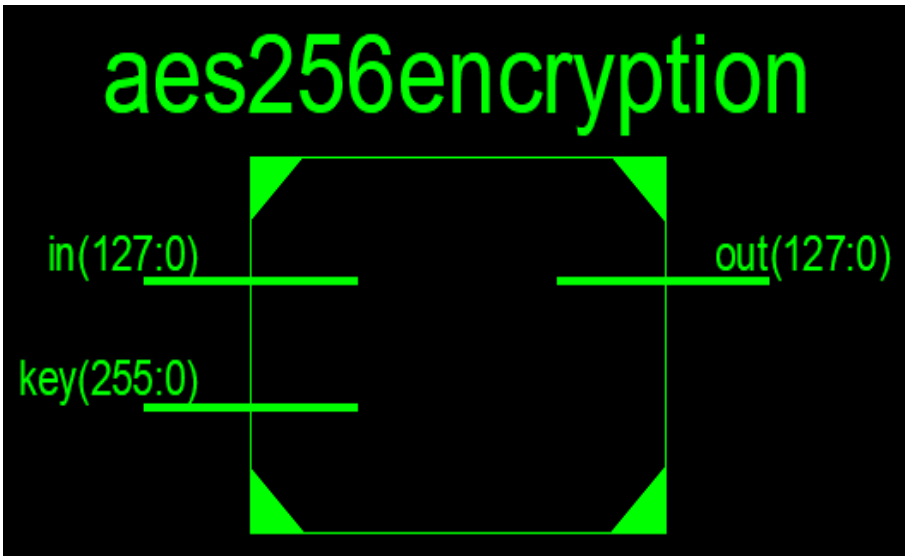

Figure 3: RTL Schematics of WiMax/IOT MAES

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 9, September 2020||

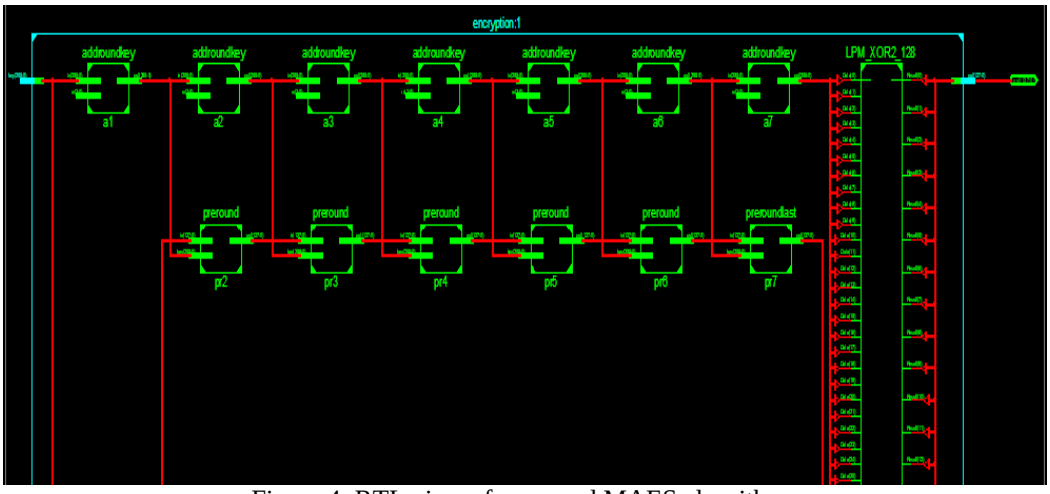

Figure 4: RTL view of proposed MAES algorithm

It is designed WiMax/IOT Security using Advanced Encryption Standard Cryptographic Algorithm. We have used Verilog for this purpose. We have used Xilinx ISE which have given synthesis results, as summarized in Table 1. Below. Also, we have depicted the pictorial representation of the results, which is the screenshot of tool generated Design Summary of individual sub-modules both at the WiMax data Encryption end and WiMax data Decryption end.

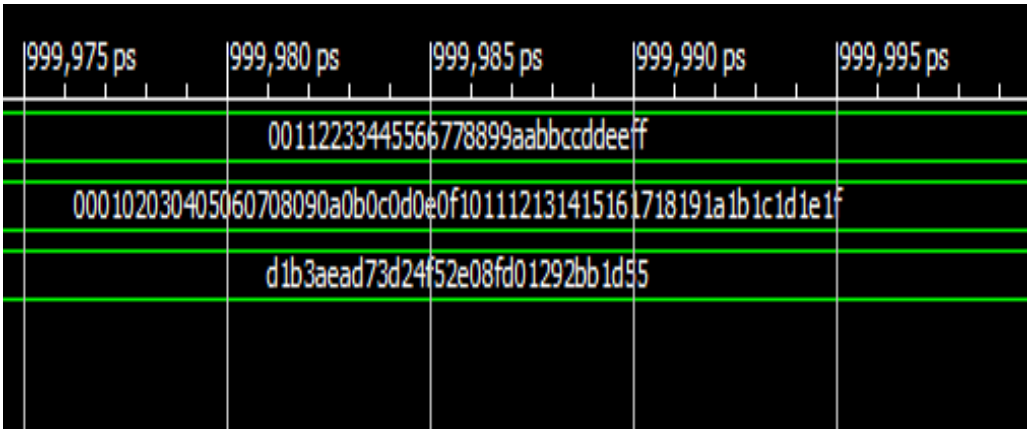

Figure 5: Encryption Process

In figure 5, firstly take 128 bit in input, in hexa form it is 00112233-445566778899aabbccddeeff. Then encrypted with secure key and generate cipher form of data.

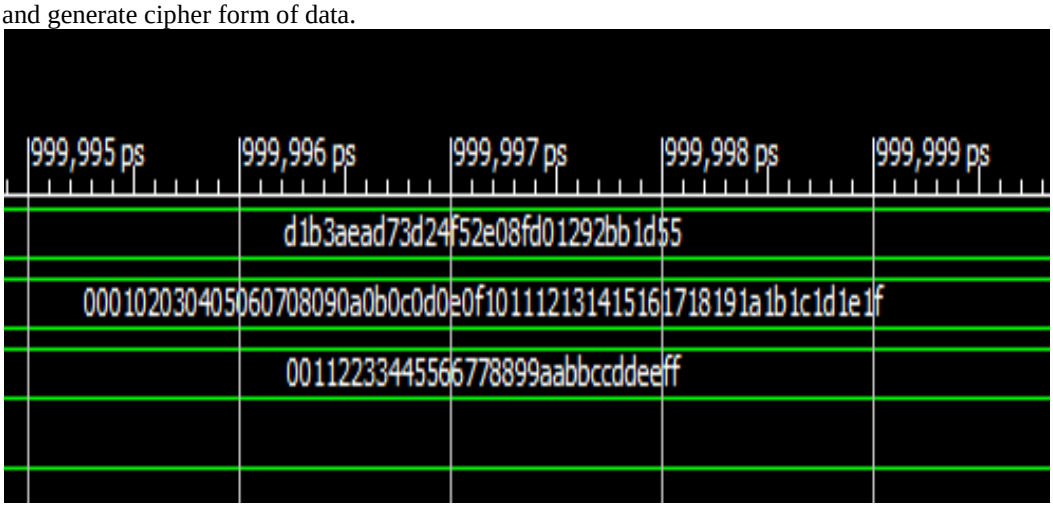

Figure 6: Decryption Process

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 9, September 2020||

In figure 6, take 128 bit in input, in hexa form it is d1b3aead73d24f524f2e08fd1292bb1d55. Then decrypted with inverse secure key and generate plain input i.e. 00112233-445566778899aabbccddeeff.

Table 1: Result Comparison of Proposed work with previous work

Sr No.	Parameters	Previous Result	Proposed Result
1	Software	nesC	Xilinx 14.7
2	Language	Structured programming	Verilog
3	Transmission time	4969.896 milli sec	2903.02 milli sec
4	Latency	29.983 milli sec	20.380 milli sec
5	Packet	1000	1000
6	Efficiency rate	18.35%	23.7%
7	Delay	29.983 milli sec	20.380milli sec
8	Voltage	1.5 V	1.2V

These comparison tables present various parameters values of previous work and proposed work. Existing work used nesC software while proposed work implemented using xilinx14.7 software. Verilog programming is used instead of structural programming. Latency, delay and transmission time is reduced than previous work. Therefore it is clear from comparison table that proposed work parameters gives significant good value than existing achieved values.
Xilinx contain various family or IC generation like Spartan, vertex kintex etc. Proposed 256 bit MAES check in various family in terms of delay, total memory, area, power and global maximum fanout. So it is clear that vertex 7 is advanced FPGA IC so it gives better outcome than other family.

V. CONCLUSION

This paper presents Modified advance encryption standard for 256 bit key with 1-D S-box. It is optimized and Synthesizable using verilog code in Xilinx software. It is developed for the implementation of both encryption and decryption process. Each program is tested with some of the random values and output results are perfect with minimal delay. Therefore, MAES can indeed be implemented with reasonable efficiency on an FPGA, with the encryption and decryption taking an average of 32 and 34 ns respectively (for every 128 bits). MAES, a lightweight version of Advanced Encryption Standard (AES) which meets the demand. A new one-dimensional Substitution Box is proposed by formulating a novel equation for constructing a square matrix in affine transformation phase of MAES. Efficiency rate of MAES is around 23.7% in terms of packet transmission which indicates MAES consumes less energy than AES, 38.117ns latency achieved and it can be applicable for Internet of Things application.

REFERENCES

1. A. R. Chowdhury, J. Mahmud, A. R. M. Kamal and M. A. Hamid, "MAES: Modified advanced encryption standard for resource constraint environments," 2018 IEEE Sensors Applications Symposium (SAS), Seoul, 2018, pp. 1-6.
2. A. Priya and R. Tiwari, “A Survey: Attribute Based Encryption for Secure Cloud”, IJOSTHE, vol. 5, no. 3, p. 12, Jun. 2018. https://doi.org/10.24113/ojssports.v5i3.70
3. S. S. S. Priya, P. Karthigai Kumar, N. M. SivaMangai and V. Rejula, "FPGA implementation of efficient AES encryption," 2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, 2015, pp. 1-4.
4. R. V. Kshirsagar and M. V. Vyawahare, "FPGA Implementation of High Speed VLSI Architectures for AES Algorithm," 2012 Fifth International Conference on Emerging Trends in Engineering and Technology, Himeji, 2012, pp. 239-242.
5. Abhiram L S, Sriroop B K, Gowrav L, Punith.Kumar H L and M. C. Lakkannavar, "FPGA implementation of dual key based AES encryption with key Based S-Box generation," 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, 2015, pp. 577-581.
6. M. El Maraghy, S. Hesham and M. A. Abd El Ghany, "Real-time efficient FPGA implementation of aes algorithm," 2013 IEEE International SOC Conference, Erlangen, 2013, pp. 203-208.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

||Volume 9, Issue 9, September 2020||

7. T. Phan, V. Hoang and V. Dao, "An efficient FPGA implementation of AES-CCM authenticated encryption IP core," 2016 3rd National Foundation for Science and Technology Development Conference on Information and Computer Science (NICS), Danang, 2016, pp. 202-205.
8. S. S. H. Shah and G. Raja, "FPGA implementation of chaotic based AES image encryption algorithm," 2015 IEEE International Conference on Signal and Image Processing Applications (ICSIPA), Kuala Lumpur, 2015, pp. 574-577.
9. S. Qu, G. Shou, Y. Hu, Z. Guo and Z. Qian, "High Throughput, Pipelined Implementation of AES on FPGA," 2009 International Symposium on Information Engineering and Electronic Commerce, Ternopil, 2009, pp. 542-545.
10. P. N. Khose and V. G. Raut, "Implementation of AES algorithm on FPGA for low area consumption," 2015 International Conference on Pervasive Computing (ICPC), Pune, 2015, pp. 1-4.
11. N. Gaur, A. Mehra and P. Kumar, "Enhanced AES Architecture using Extended Set ALU at 28nm FPGA," 2018 5th International Conference on Signal Processing and Integrated Networks (SPIN), Noida, 2018, pp. 437-440.
12. J. Senthil Kumar and C. Mahalakshmi, "Implementation of pipelined hardware architecture for AES algorithm using FPGA," 2014 International Conference on Communication and Network Technologies, Sivakasi, 2014, pp. 260-264.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.512

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details