International Journal of Engineering Research & Management Technology ISSN: 2348-4039

March- 2015 Volume 2, Issue-2

Email: editor@ijermt.org www.ijermt.org

Security Driven Data Aggregation in Mobile Sensing

Dinesh Kumar
Department of Information Technology
SRM University, NCR Campus
Modinagar, Ghaziabad, India

Parisha Raj ,Varsha Shokeen
Department of Information Technology
SRM University, NCR Campus
Modinagar, Ghaziabad, India

ABSTRACT:
With the ever increasing demand and advancement of mobile devices such as smart phones giving rise to number of mobile sensing technologies which collect data form embedded sensors of mobile devices. These sensors are applied to various tasks like environmental monitoring, traffic monitoring, healthcare etc.. But with ever increasing use of mobile sensing application is disrupted by several challenges like privacy leakage from sensing data, lack of mobile user participation, and lack of security mechanism for collection of data.
The specific goal is to provide a way how sensor data can be protected at client site. We achieve this goal by providing encryption with the intent of mobile user that which document he wish to protect from other. Only those whom he want to share data can sense the required data and entrusted user are kept away from sensing data. They also ensure that dishonest users cannot abuse the system to earn unlimited credits. Only trusted servers can access the system. To provide effective privacy we design a DES based encryption scheme which allow mobile user to self access the encryption method and decide the limit of protection in their mobile system.
Keyword: mobile sensing, DES algorithm, client side, aggregator, threat.

I. INTRODUCTION

Mobile sensing is increasingly becoming part of everyday life due to the rapid evolution of the mobile phone into a powerful sensing platform. Popular consumer Smartphone are now equipped with the necessary sensors to monitor a diverse range of human activities and commonly encountered contexts like GPS, camera, microphones. The technical challenges of mobile sensing have attracted interest from various research communities, such as experts in machine learning, human computer interaction and mobile systems, who approach this emerging field with their own perspective due to differences in their interests and expertise. Mobile sensing application relies on small number of volunteers hence data is limited. The large scale of deployment of data are affected by lack of participation of mobile users because it leads to high cost of mobile data as well as it consume much power of the device and privacy consent of user.
In this paper we explain DES cryptographic algorithm. And we will focus on how encryption of data can be done at client site.

II. LITERATURE REVIEW

The relevant literature review is mentioned as follows:

Serial No.	Paper title	Description
1	Providing Efficient Privacy-Aware Incentives for Mobile Sensing	Privacy aware incentive scheme for general mobile sensing, which allows each sensing task to collect one or multiple reports from each user as needed
2	Secure and Privacy-Aware Sensor Networks Data Collection in Wireless	a layered key distribution scheme together with two protocols for query authentication and confidential data aggregation

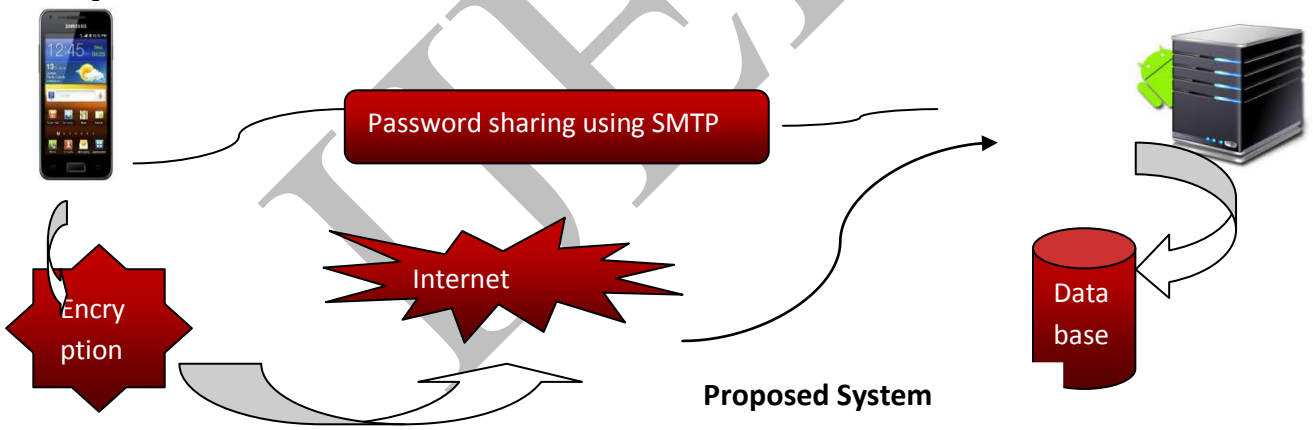
III. EXISTING PROBLEM

The present mobile sensors share the data on global basis. User is unable to decide which data he wants to keep secure from entrusted users. Little bit of encryption is done at server site but till then all the sensor data is globally distributed. Thus compromising the privacy of user. The decryption round at server site takes an extra round of interaction between clients and server. The present system takes high computation cost together with high storage memory.

Existing System

IV. PROPOSED SYSTEM

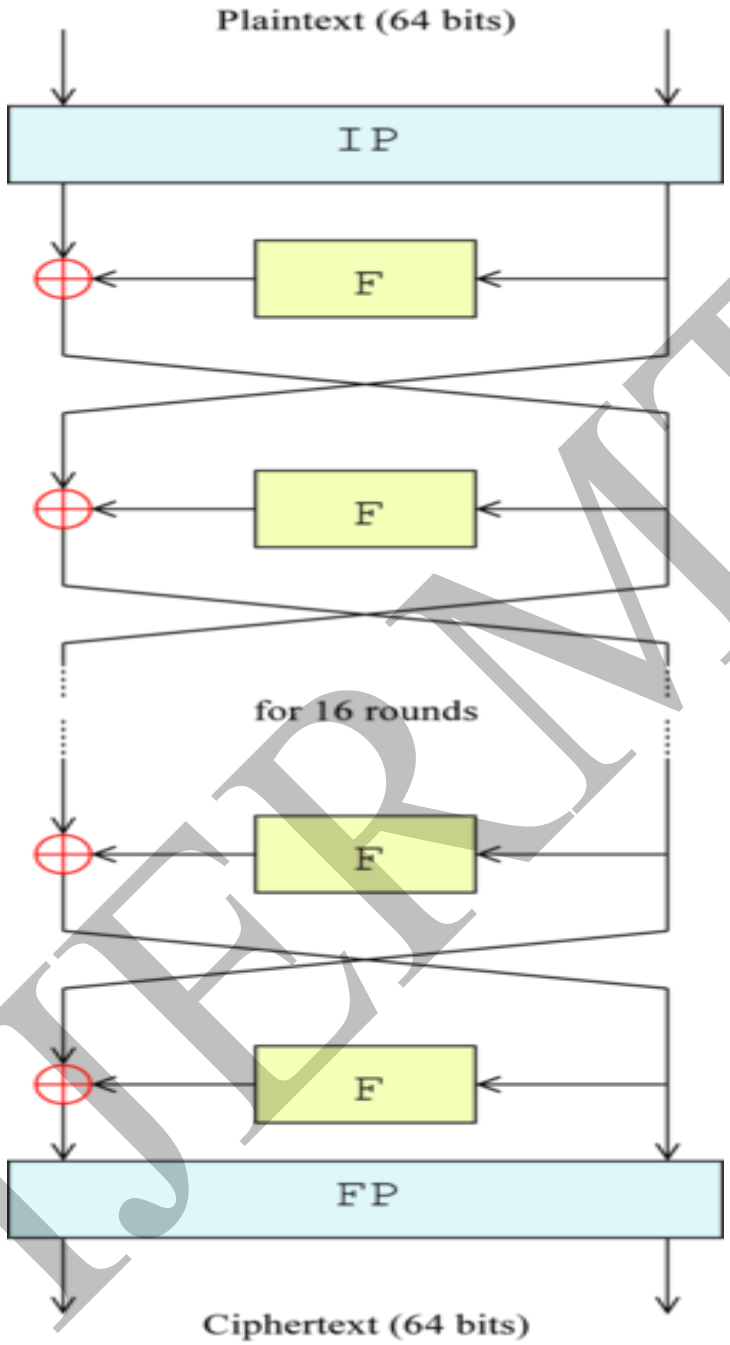
Thus to eliminate the problem of privacy concern, high computation cost and extra round of interaction between the mobile user and the server, we propose a system which uses the DES encryption algorithm at the client site i.e. the user himself decide which data is required to be encrypted and which can be left to global server. There is no requirement of any interaction between mobile user and the trusted server. Only interaction is if user want o change its personal information or password related queries with the trusted server. All the aggregator can only access those data which are available on mobile device. Even if an aggregator tries to download encrypted data it will get downloaded but in unreadable format. Only the document can be opened if respective password is used to open it. Wrong password will lead no information for aggregator. If user wants to share his data with some trusted aggregator then the password related to that document is shared using SMTP protocol.



Proposed System

V. DES ALGORITHM

Data Encryption Standard – data are encrypted using 64- bit data and 56-bit key. .The algorithm transforms 64-bit input in a series of steps into a 64-bit output. The same steps, with the same key, are used to reverse the encryption.



The processing of the plaintext proceeds in three phases. First, the 64-bit plaintext passes through an initial permutation (IP) that rearranges the bits to produce the permuted input. This is followed by a phase consisting of sixteen rounds of the same function, which involves both permutation and substitution functions. The output of the last (sixteenth) round consists of 64 bits that are a function of the input plaintext and the key. The left and right halves of the output are swapped to produce the pre output. Finally, the pre output is passed through a permutation that is the inverse of the initial permutation function, to produce the 64-bit cipher text. With the exception of the initial and final permutations; DES has the exact structure of a Feistel cipher. The 56-bit key is used..Initially, the key is passed through a permutation function. Then, for each of the sixteen rounds, a sub key ( ) is produced by the combination of a left circular shift and a permutation. The permutation function is the same for each round, but a different sub key is produced because of the repeated shifts of the key bits

***(a)* Initial Permutation**

IP

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

***(b)* Inverse initial permutation**

IP^{-1}

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

***(c)* Expansion Permutation**

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	28
24	25	26	27	28	29
28	29	30	31	32	1

***(d)* Permutation Function**

16	7	20	21	29	12	28	7
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

Details of single Round- The left and right halves of each 64-bit intermediate value are treated as separate 32-bit quantities, labelled L (left) and R (right).As in any classic Feistel cipher, the overall processing at each round can be summarized in the following formulas:

$L_i=R_{i-1}$

$R_i=L_{i-1} \text{ xor} F(R_{i-1},K_i)$

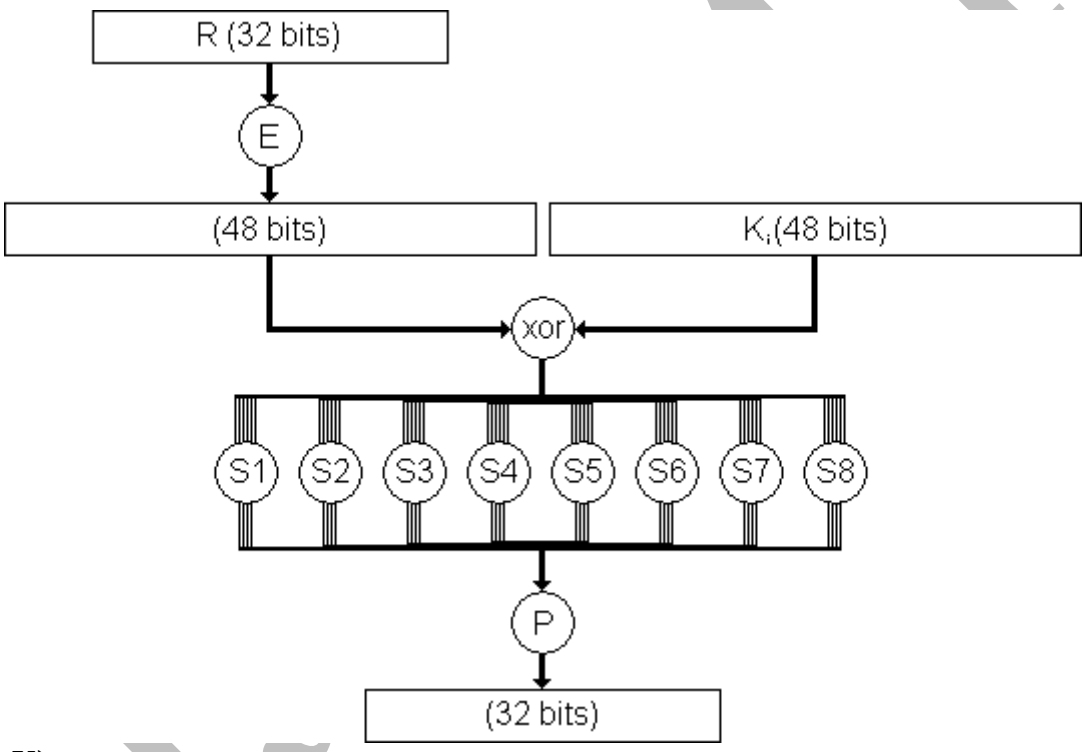
The round key is 48 bits. The input is 32 bits. This input is first expanded to 48 bits by using a table that defines a permutation plus an expansion that involves duplication of 16 of the bits .The resulting 48 bits are XORed with. This 48-bit result passes through a substitution function that produces a 32-bit output, which is permuted as defined by. The role of the S-boxes in the function F. The substitution consists of a set of eight S-boxes, each

of which accepts 6 bits as input and produces 4 bits as output. These transformations are defined in , which is interpreted as follows: The first and last bits of the input to box form a 2-bit binary number to select one of four substitutions defined by the four rows in the table for . The middle four bits select one of the sixteen columns. The decimal value in the cell selected by the row and column is then converted to its 4-bit representation to produce the output. For example, in S1, for input 011001, the row is 01 (row 1) and the column is 1100 (column 12).The value in row 1, column 12 is 9, so the output is 1001. Each row of an S-box defines a general reversible substitution. May be useful in understanding the mapping. The figure shows the substitution for row 0 of box. The operation of the S-boxes is worth further comment. Ignore for the moment the contribution of the key ( ).If you examine the expansion table, you see that the 32bits of input are split into groups of 4 bits and then become groups of 6 bits by taking the outer bits from the two adjacent groups. For example, if part of the input word is

...efgh ijkl mnop....

This becomes

...defghi hijklm lmnopq



Calculation of F(R,K)

The outer two bits of each group select one of four possible substitutions (one row of an Sbox).Then a 4-bit output value is substituted for the particular 4-bit input (the middle four input bits). The 32-bit output from the eight S-boxes is then permuted, so that on the next round, the output from each S-box immediately affects as many others as possible.

Key Generation-A 64-bit key is used as input to the algorithm. The bits of the key are numbered from 1 through 64;every eighth bit is ignored .The key is first subjected to a permutation governed by a table labelled Permuted Choice One .The resulting 56-bit key is then treated as two 28-bit quantities. At each round, and are separately subjected to a circular left shift or (rotation) of 1 or 2 bits. These shifted values serve as input to the next round. They also serve as input to the part labelled Permuted Choice Two , which produces a 48-bit output that serves as input to the function.

Permuted Choice 1

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	21	4

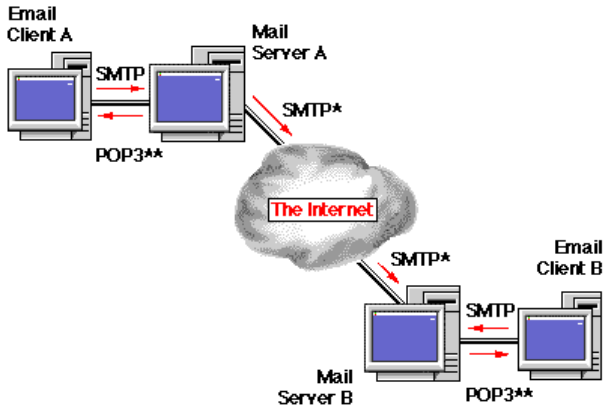
Permuted Choice 2

14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	47	44	49	39	56
34	53	46	42	50	36	29	32

VI. SMTP-SIMPLE MAIL TRANSFER PROTOCOL

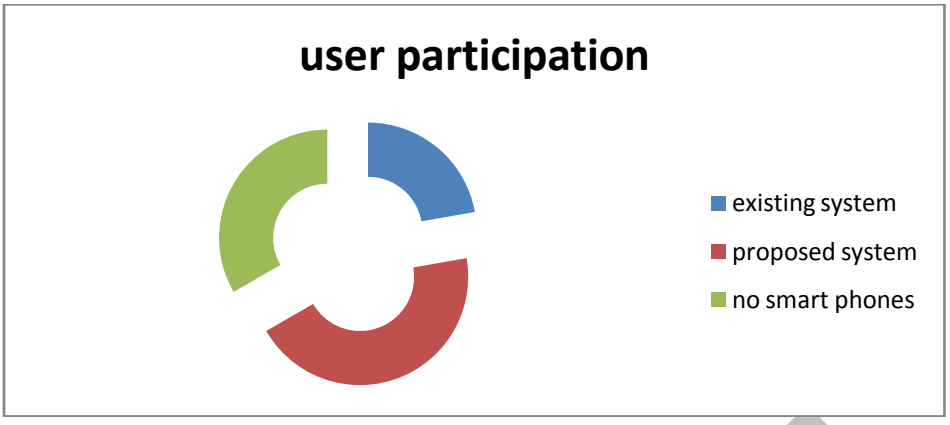
SMTP is a n internet standard for electronic mail transmission. SMTP by default uses TCP port 25. The protocol for mail submission is same but uses port 587.SMTP is secured by SSL, by default port is 465.

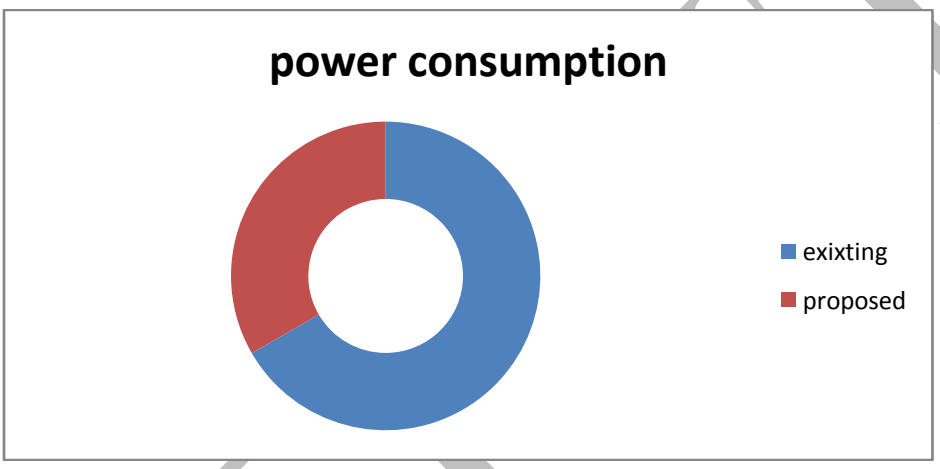
Although electronic mail servers and other mail transfer agents use SMTP to send and receive mail messages, user-level client mail applications typically use SMTP only for sending messages to a mail server for relaying. For receiving messages, client applications usually use either POP3 or IMAP.



VII. DATA ANALYST REPORT

Comparing the data of existing system and proposed one , we analysed that the participation of user has increased from 20% to 40% approximately. As the new system cost low 3Gplan as well as power consumption of mobile devices will be low. Together with these mobile users will not require being in touch with the server or the aggregator all the time. These benefits of proposed system will increase its utilization.





VIII. FUTURE SCOPE

The proposed system can be used very effectively. Some drawbacks are recently only document files are being encrypted. Later with the advancement of cryptographic technology like replacing DES algorithm with higher and advanced technology will allow us to encrypt pictures videos audios etc.. Present in our mobile devices.
And mobile devices with OS like windows apple android can use it and embed the application in their devices.

IX. CONCLUSION

Thus the proposed system is far better than the existing system with respect to the amount of storage area, power consumption, internet usage and round of interaction between the aggregator and the mobile user.
When the little drawbacks of the proposed system will be removed then it will be used by more users. A new network solution company named Spring Network Solution has started the innovation like the proposed system named SILVER SPRING NETWORK.

X. REFERENCES

1. Cryptography and Network Security- Principles and Practices, Fourth Edition, William Stallings.
2. Providing Privacy-Aware Incentives for Mobile Sensing by Qinghua Li, Guohong Cao
3. Supporting Mobile Privacy and Security through Sensor-Based Context Detection by Julian Seifert Bauhaus-University Weimar
4. A survey of mobile phone sensing by Nicholas D. Lane, Emiliano Miluzzo, Hong Lu, Daniel Peebles, Tanzeem Choudhury, and Andrew T. Campbell, Dartmouth College
5. Springnet Solutions