ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 9, Issue 1, pp: (107-116), Month: January - March 2021, Available at: www.researchpublish.com

RANDOM NUMBER GENERATOR BASED ON C++

Yazeed Al Moaiad [1], Wafa Al-Haithami[2]

Al-Madinah International University, Malaysia

[1]yazeed.alsayed@mediu.edu.my

[2]wafaaalhithmy@yahoo.com

Abstract: **Identify the random number generator and its security will be important. Determining how to improve the security of communication cards by random numbers generator. Reasons are given why random number generators should be done using analytically mathematical and programming. Doing the program of the random number generators is intensive. The discussion in the research aims to prove that whether the system is valid or invalid. One of the main of part common uses of Random Number Generators for recharge communication and credit cards. There is a relationship between the serial number and the secret number in the same credit card. Also, the secret number consists of fourteen numbers, part of them is as a part of the serial number in the same card. Nowadays, they are aware of the importance of cellular phones in our daily life. Then, they want to discover a new and effective way to decrease the effect of the security issue and increase protection. Most communication firms based on random number generators (RNGs) programs to recharge communication cards, but the essential problem has its security level for that cards, in which the hackers will decrypt the secret number by some hacking programs simply. The security of most systems relies on unpredictable and irreproducible keys using a non-deterministic random number generator. Therefore, using the analytically mathematical method and programming language for random number generation like C++ language may improve the security level which is being used for communication and credit cards.**

Keywords: **Random Number Generator, Serial Number, Secret Number, Credit Card.**

I. INTRODUCTION

Identifying the random number generator and its security. Determining how to improve the security of communication cards by random numbers generator. Reasons are given why random number generators should be done using analytically mathematical and programming. Doing the program of the random number generators is intensive. The discussion in the research aims to prove that whether the system is valid or invalid. Cellular phones are considered the most popular way of communication around the world which It has changed the way people communicate with one another more than anything since the invention of the telephone more than a century ago. The success of these new methods of communication is demonstrated. [1] and [5].

During the last decade, the number of cellular phones is increased, and the success of most telecommunications companies is still related and affected by data security issue concerns where some type of protection is required. Nowadays, they are aware of the importance of cellular phones in our daily life. Then, they want to discover new and effective ways to decrease the effect of the security issue and increase protection. Most communication firms based on random number generators (RNGs) programs to recharge communication cards, but the essential problem has its security level for that cards, in which the hackers will decrypt the secret number by some hacking programs simply. The security of most systems relies on unpredictable and irreproducible keys using a non-deterministic random number generator. Therefore, using the analytically mathematical method and programming language for random number generation like C++ language which may improve the security level which is being used for communication and credit cards. [2] and [6].

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 9, Issue 1, pp: (107-116), Month: January - March 2021, Available at: www.researchpublish.com

II. PROBLEM STATEMENT

One of the main of part common uses of Random Number Generators for recharge communication and credit cards. The research problem will concern communication cards as follow:

There is a relationship between the serial number and the secret number in the same credit card. Also, the secret number consists of fourteen numbers, part of them is as a part of the serial number in the same card.

As a result of that, the actual secret number of a card will be reduced and becomes only around six numbers instead of fourteen numbers. The following figure shows the relationship between the serial number and the secret number in the same credit card, which are related to MTN company in Yemen. [3]

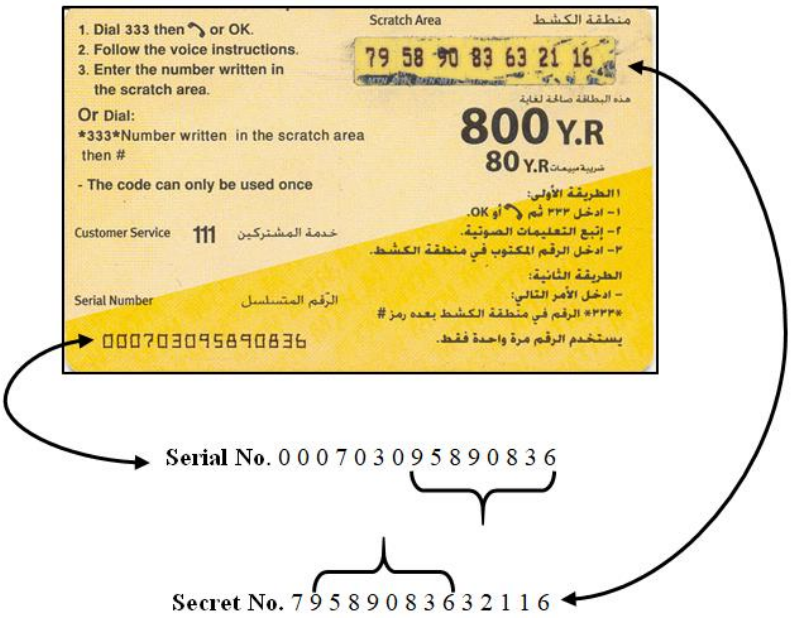

FIGURE 1A: THE RELATIONSHIP BETWEEN SECRET NO. AND SERIAL NO.

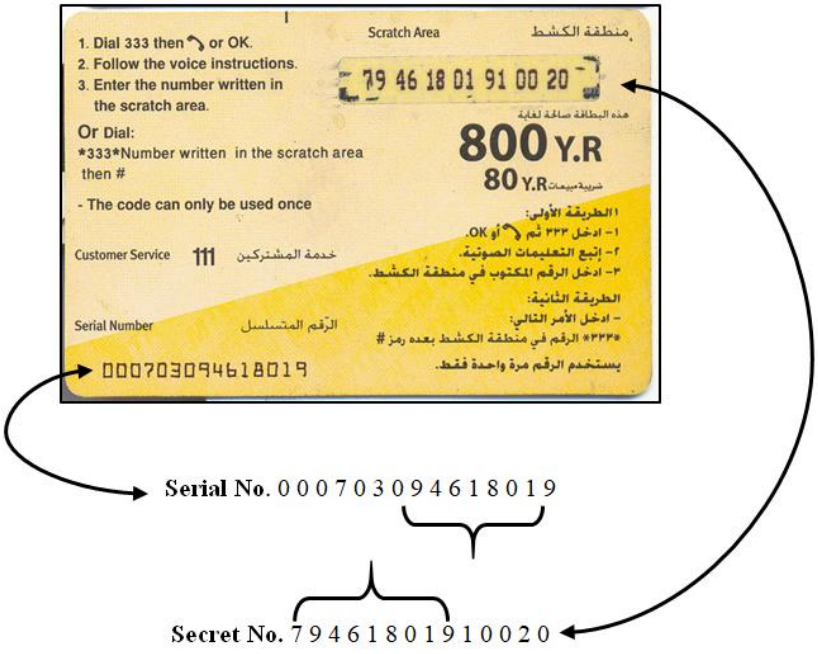

FIGURE 1B: THE RELATIONSHIP BETWEEN SECRET NO. AND SERIAL NO.

One could find the same numbers at least eight numbers in secret and serial numbers card that will be easiest to decode of the secret number by hackers.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 9, Issue 1, pp: (107-116), Month: January - March 2021, Available at: www.researchpublish.com

III. OBJECTIVES OF THE STUDY

1. Identifying the random of numbers generator and its security.
2. Determining how to improve the security of communication cards by random of numbers generator.
3. Doing the program of the random number generators is intensive. The discussion in the research aim to prove that whether the system is valid or invalid.

IV. METHOD

It involves general research perspectives, purpose, approach, data collection, and research credibility.

A. Research Perspectives

In this research the general perspective is formulated by insertion a secret key with subset length. An algorithm which uses one-way hash function to generate substitution boxes used to generate random numbers and protect the used secret key.

B. Research Purpose

The research purpose is generating random numbers used as a protection approaches in communication cards. Also, in this research, the purpose is to remove the relationship between the serial and secret number which used in the communication cards.

C. Research Approach

In this research dynamic substation boxes are generated base on secret key, which in turn used to generate random numbers in one-way hash function. The generated random numbers are used in the communication cards as a protection tool.

D. Research Strategy

In this research, mode operation with two-dimension matrixes, along with permutation (substitution boxes) functions, conversion functions are used to generate random numbers from binary to decimal numbers and vice versa.

E. Data Collection

In this section it will be intended to decide the method that will be planned to go through specific purpose of addressing the research problem.

The data was collected from:

- Investigation:

1. Checking the cards that are available in the market.

2. There is security violation such as breaking cards.

3. By interview.

- Interview:

Interviewed with an owner of a telecommunication shop and a sales manager of a telecommunication company to get some information about scratch cards.

V. RESULT AND DISCUSSION

The most important stage of the system because it proves whether the system is valid or invalid. It will discuss the following:

The Detailed Study of the System.

A. Reanalyzing Research Problem

The problem is restated in details and one could show the relationship between secret number and serial number that are shown in figure 1.1, (a) and (b), and appear directly the relationship between secret and serial numbers. As a result, the

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 9, Issue 1, pp: (107-116), Month: January - March 2021, Available at: www.researchpublish.com

actual secret number of a card will be reduced and becomes only six numbers instead of fourteen numbers that will be easiest to decode by hackers.

Now, after showing the relationship between them, our program is going to solve the determined problem by using mixed three types RNGs to generate random number. [4]

As a result, there is no relationship between secret and serial numbers. this is a sample of the result, which is pointed in figure 2.

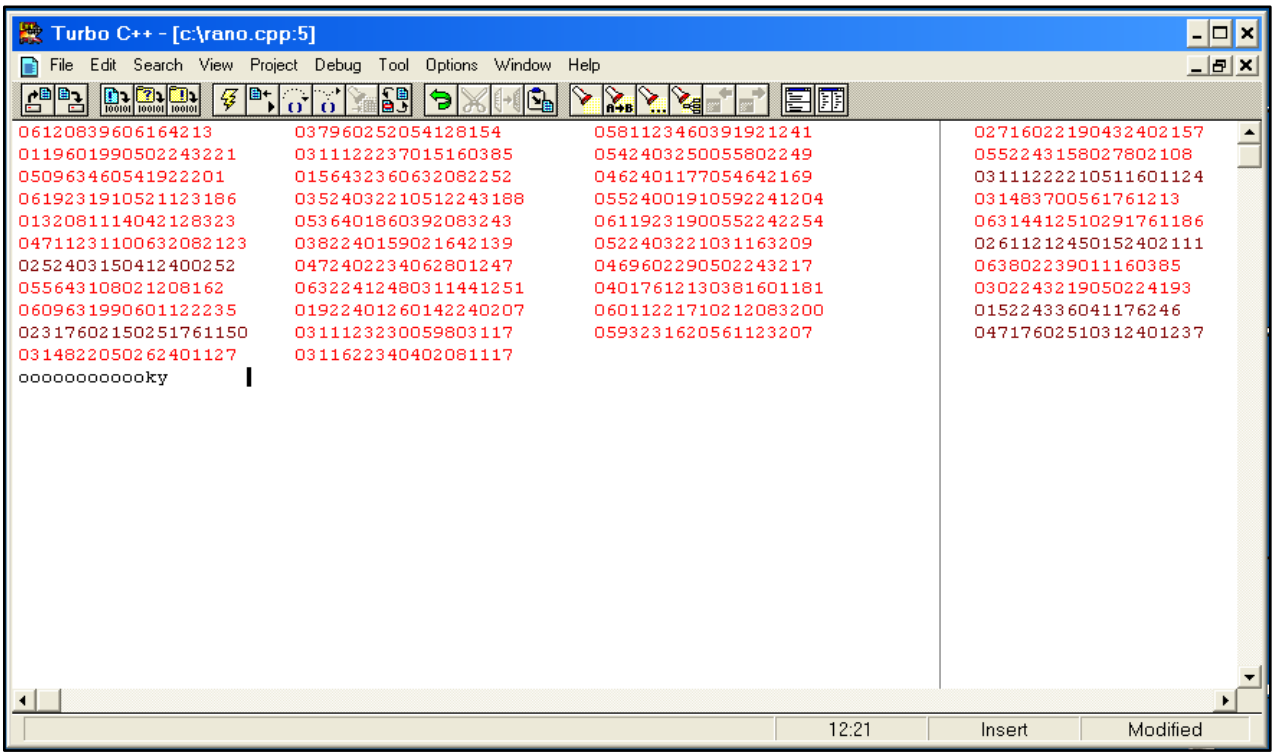

FIGURE 2: SECRET RANDOM NUMBERS

For instance, when taking sample of secret numbers, the first secret random number (06120839606164213) and use number one (1) as a serial number. Absolutely, there is no relationship between secret and serial numbers. Another sample, the tenth secret random number is (0156432360632082252) and using number ten (10) as a serial number. the same result will be gotten.

B. Entity and Relationship Diagrams

1. Cards Entity:

This screen shows the cards entity which is consist of three main elements card state, Secret number, and Serial number. All elements type of number.

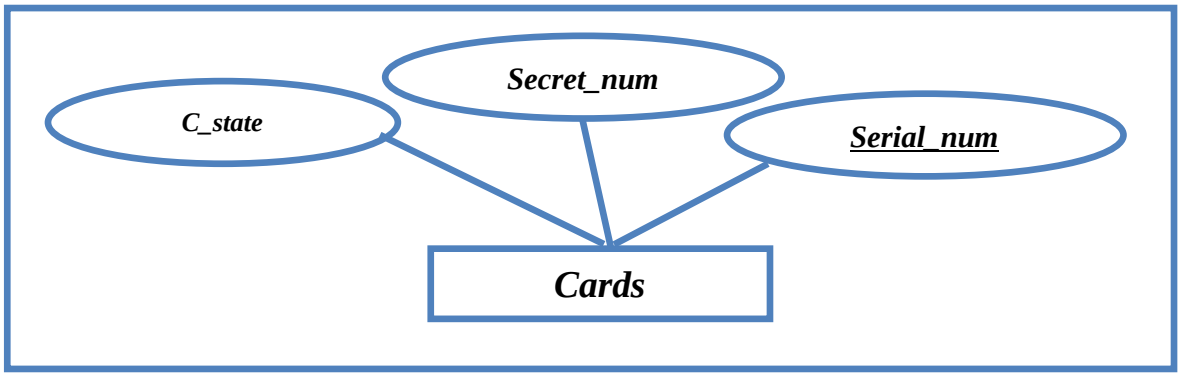

FIGURE 3: CARDS ENTITY

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 9, Issue 1, pp: (107-116), Month: January - March 2021, Available at: www.researchpublish.com

C. User Entity

As following below, user's entity has four elements password its type is char, user state its type is number, user name its type is char and user number its type is number.

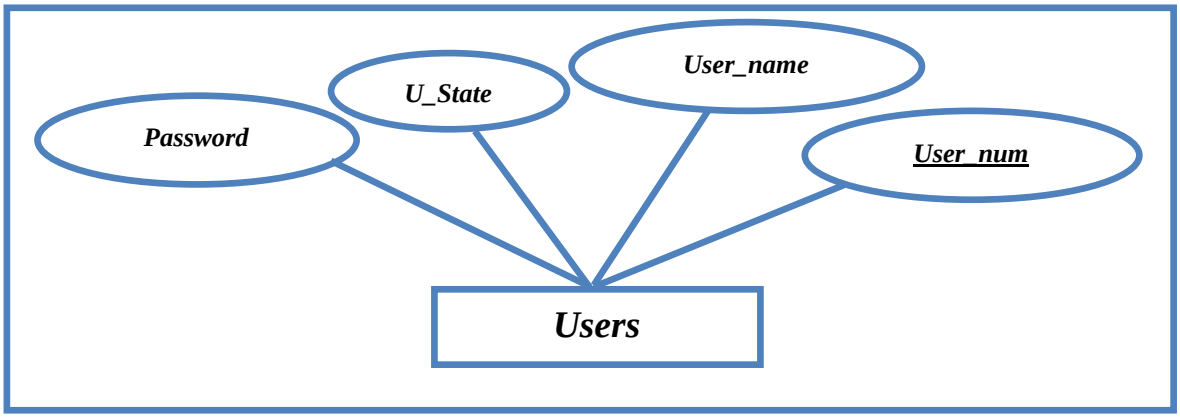

FIGURE 4: USERS' ENTITY

D. Units Type Entity

Units type Entity are company, and its type is char, unit type number its type is number, and unit type its type is char.

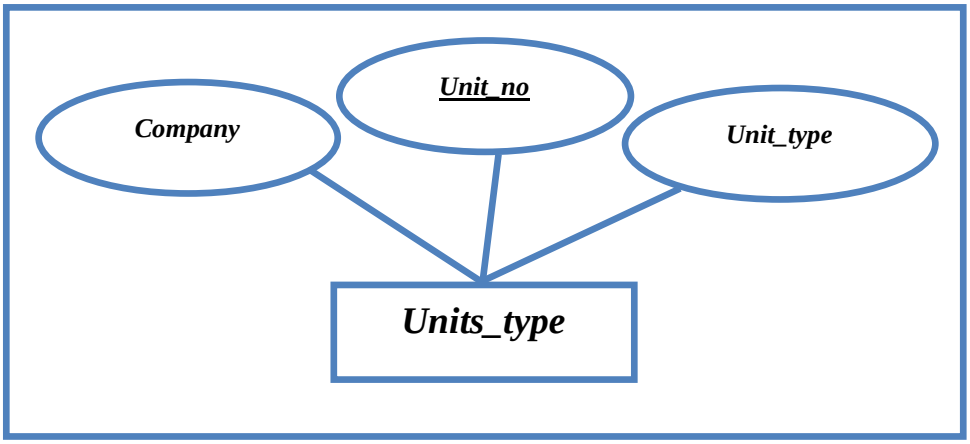

FIGURE 5: UNITS TYPE ENTITY

E. Units Value Entity

This screen shows Units value Entity its elements are cost, value and ID all of them are type of numbers.

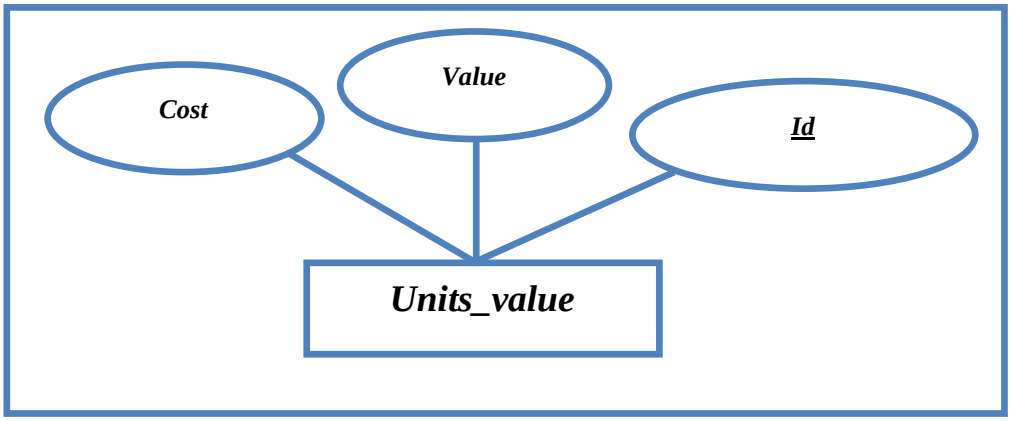

FIGURE 6: UNITS VALUE ENTITY

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 9, Issue 1, pp: (107-116), Month: January - March 2021, Available at: www.researchpublish.com

F. Privileges Entity

These are two elements of Privileges Entity, privilege number its type is number, and privilege type its type is char which is given for entities.

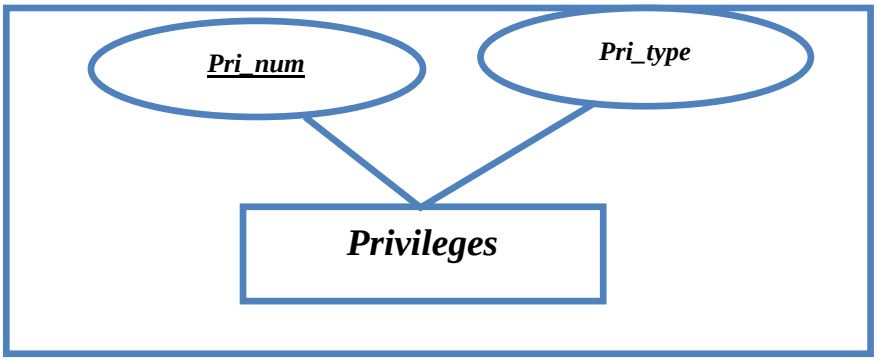

FIGURE 7: PRIVILEGES ENTITY

G. Relationships Diagram

This screen shows the kind of relationships. For example, one to one or one to many and many to many.

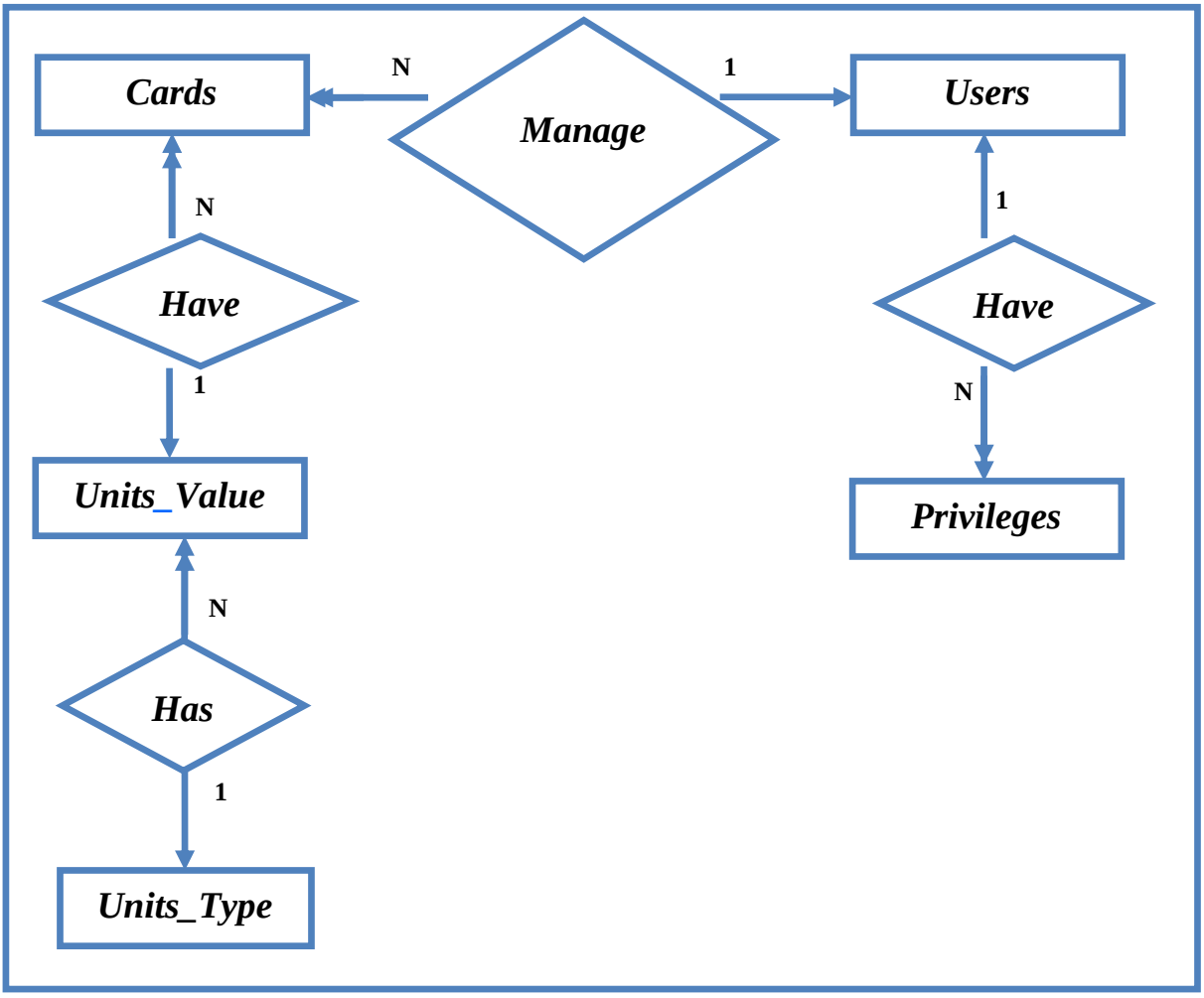

FIGURE 8: RELATIONSHIPS DIAGRAM

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 9, Issue 1, pp: (107-116), Month: January - March 2021, Available at: www.researchpublish.com

H. Data Flow Diagram (DFD)

In the phase will be describing the following:

1. Data Flow Diagram:

In the phase will be describing the following:

2. Context Diagram:

This defines the relation between the system and the environment that is a round it.

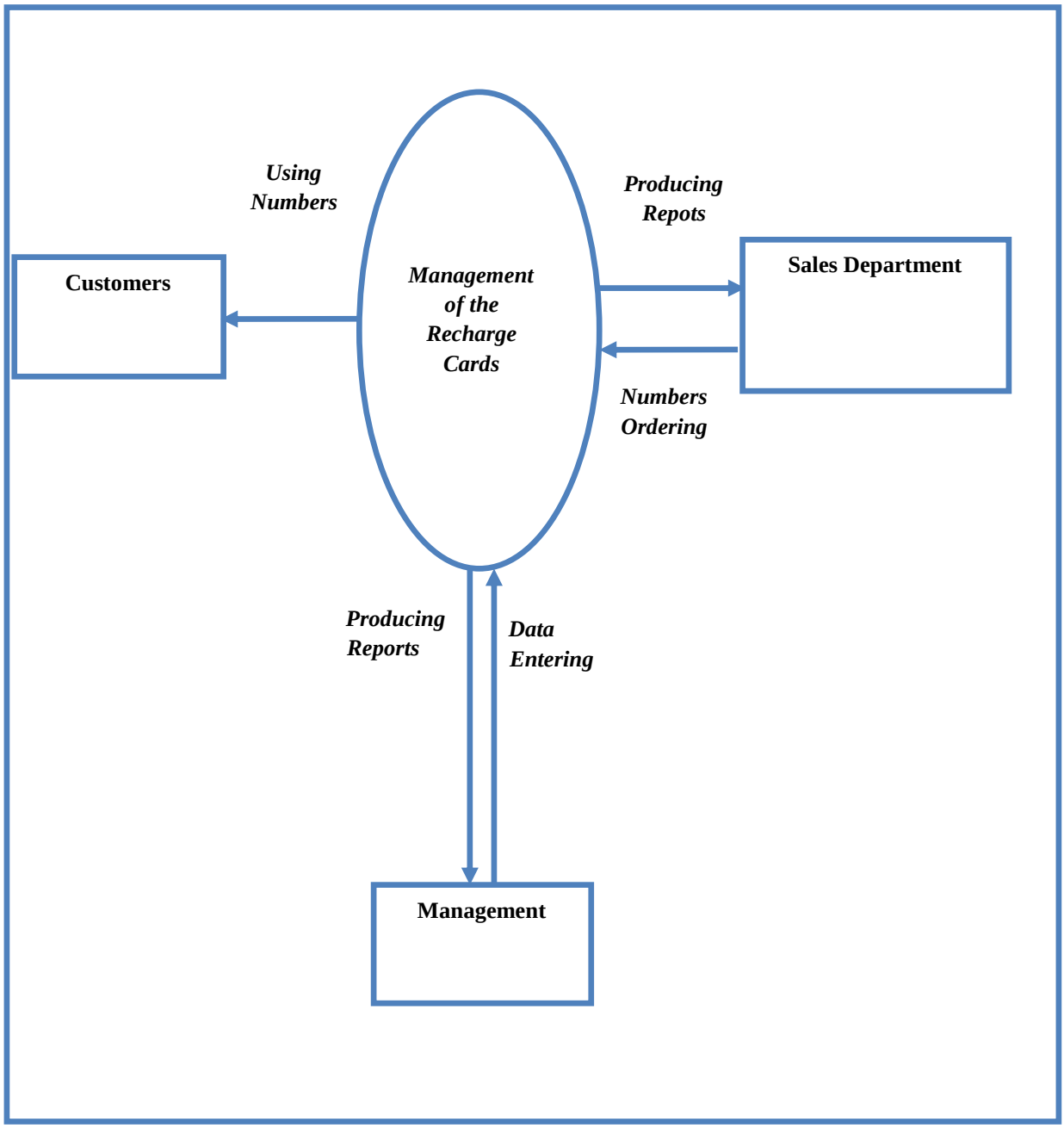

FIGURE 9: CONTEXT DIAGRAM

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 9, Issue 1, pp: (107-116), Month: January - March 2021, Available at: www.researchpublish.com

I. General Diagram

This screen describes the main relation and identifies the relation between different processes.

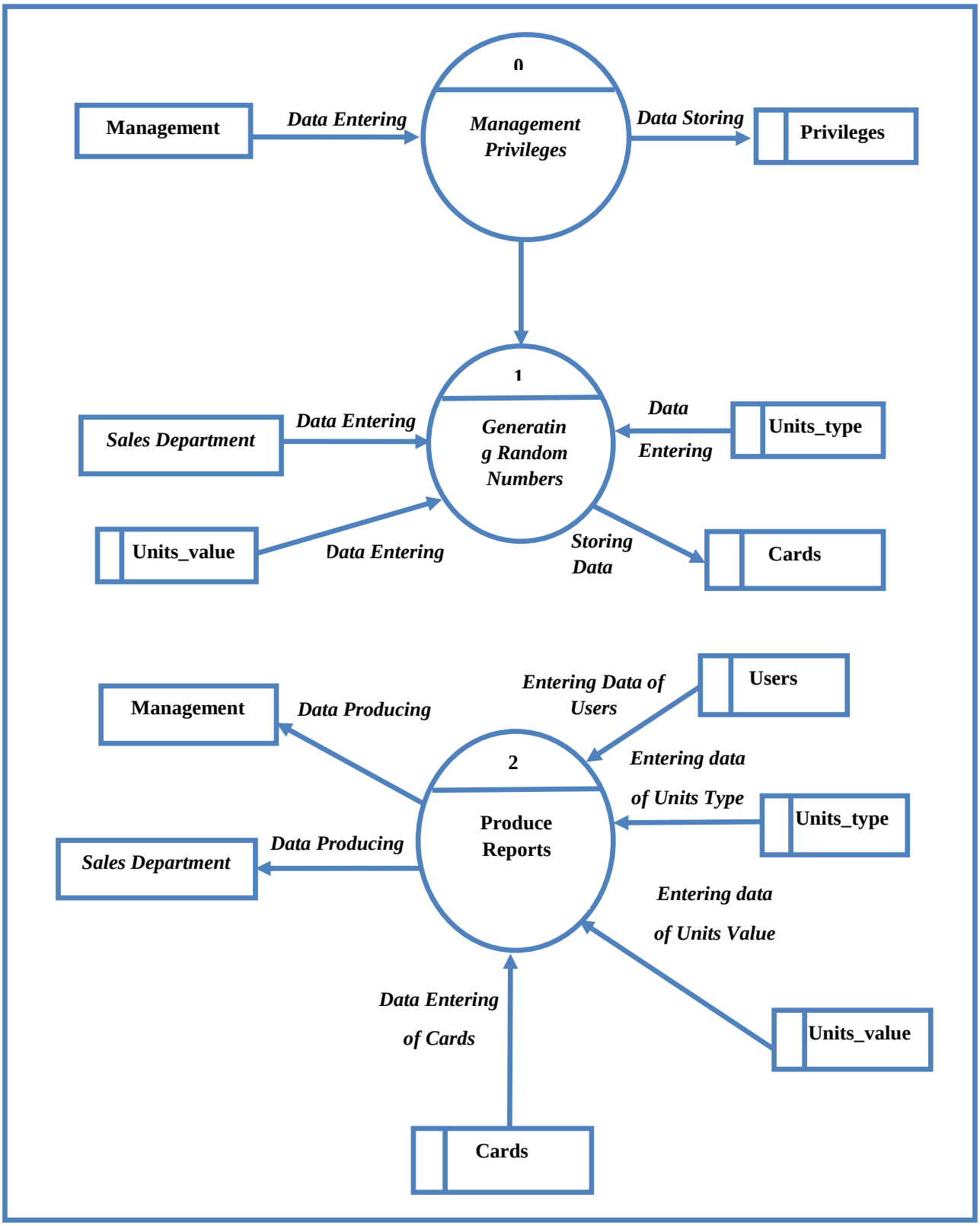

FIGURE 10: GENERAL DIAGRAM

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 9, Issue 1, pp: (107-116), Month: January - March 2021, Available at: www.researchpublish.com

- The details diagram of management privileges process.

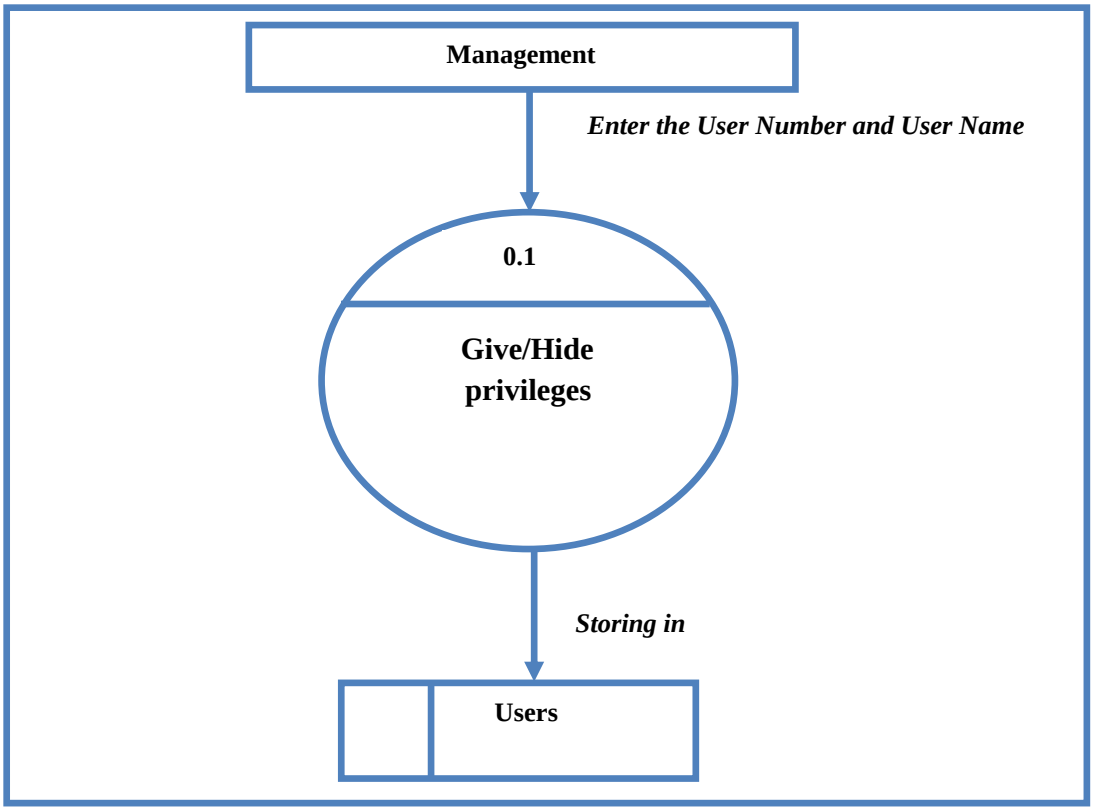

FIGURE 11: MANAGEMENT PRIVILEGES PROCESS

J. Data Dictionary

This phase will describe the data elements:

TABLE 1: DESCRIBING OF THE DATA ELEMENT

Number	*Name of Data Elements*	*Programming Name*	*Type*	*Size*	*A place to be used*
1	Serial Number	Serial_num	Number	16	Cards
2	Secret Number	Secret_num	Number	26	Cards
3	Card State	C_state	Number	1	Cards
4	User Number	User_num	Number	4	Users
5	User Name	User_name	Char	30	Users
6	Password	password	Char	12	Users
7	User State	U_State	Number	1	Users
8	Privileges Number	Pri_num	Number	2	Privileges
9	Privileges Type	Pri_type	Char	20	Privileges
10	Units type Number	Unit_no	Number	2	Units_type
11	Units Type	Unit_type	Char	10	Units_type
12	Company	Company	Char	20	Units_type
13	Value Number	Id	Number	2	Units_value
14	Value	Value	Number	10	Units_value
15	Cost	Cost	Number	10	Units_value

VI. CONCLUSION

In this research, the successful in constructing a simple and small system for telecommunication firms by using analytically mathematical and programming. Our design is simple, straightforward and the feasibility of the system has been studied according to a financial and technical aspects. The research is successful in analyzing the reasons of the research problems. It reviewed all the techniques, which related to random number generators. With emphasis on the three well-known RNG primitives, which are True, Pseudo and Quasi random number generators.

REFERENCES

[1] Yassein, M. B., Aljawarneh, S., Qawasmeh, E., Mardini, W., & Khamayseh, Y. (2017, August). Comprehensive study of symmetric key and asymmetric key encryption algorithms. In 2017 international conference on engineering and technology (ICET) (pp. 1-7). IEEE.

[2] Kneusel, R. T. (2018). Testing Pseudorandom Generators. In Random Numbers and Computers (pp. 115-158). Springer, Cham.

[3] de la Fraga, L. G., Torres-Pérez, E., Tlelo-Cuautle, E., & Mancillas-López, C. (2017). Hardware implementation of pseudo-random number generators based on chaotic maps. Nonlinear Dynamics, 90(3), 1661-1670.

[4] Buchovecka, S., Lórencz, R., Kodýtek, F., & Buček, J. (2017). True random number generator based on ring oscillator PUF circuit. Microprocessors and Microsystems, 53, 33-41.

[5] Kneusel, R. T. (2018). Random numbers and computers (Vol. 239). Cham, Switzerland: Springer.

[6] Acosta, A. J., Addabbo, T., & Tena-Sánchez, E. (2017). Embedded electronic circuits for cryptography, hardware security and true random number generation: an overview. International Journal of Circuit Theory and Applications, 45(2), 145-169.

[7] Yu, F., Li, L., Tang, Q., Cai, S., Song, Y., & Xu, Q. (2019). A survey on true random number generators based on chaos. Discrete Dynamics in Nature and Society, 2019.