IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 7, July 2021

DOI: 10.17148/IARJSET.2021.8731

SECURE FUND TRANSFER OVER INTERNET USING AES ALGORITHM

Akash Suryawanshi [1], Aryan Saxena[2], Astha Agnihotri[3], Diksha Singh[4]

Assistant professor, Department of Computer Engineering, Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune, India-411043[1]

Department of Computer Engineering, Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune, India-411043[2, 3, 4]

Abstract: Nowadays human beings frequently need to transfer coins from one account to another. In such instances they want to visit bank or look for computer linked to net to get admission to the services supplied with the aid of net banking for reliable fund switch. This system proves to be without a doubt beneficial in such cases. As with the assist of this device the user just needs to enter the account information. For security, AES algorithm is used together with immediately verification and consistency check algorithm. These types of are performed for secure electronic fund transfer. For this reason, a person just wishes to visit any EFT centre, so that you can make the price. The transfer is done instantly the use of a single portable card. In this manner the user can make the fee securely as this device uses DES for protection and the switch is being accomplished right away. As quickly as the consumer card is scanned, it gets a SMS message. SMS includes OTP that's particular. All of the person needs to do is enter this OTP received which will increase stage of protection. After OTP the person needs to go into account info. This information is being encrypted using AES earlier than sending it over the community. Consequently, this gadget guarantees safety for electronic fund transfer the usage of AES. Current economic establishments have cashed in at the electronic business possibilities of the internet by using growing severe fee systems to satisfy diverse price provider requirements.

Keywords: AES, DES, OTP, Encryption, EFT.

INTRODUCTION

The origin of the electronic assets exchange (EFT) industry can be taken after back to the presentation of the at first robotized teller machine (ATM) in the mid-1960s. The ATM could manage record exchanges, recognize stores, and oversee cash using a standard appealing stripe card and individual unmistakable confirmation number (PIN). With the presentation and affirmation of ATMs, U.S. budgetary establishments entered the time of EFT systems. The term EFT insinuates the usage of PC and telecom advancement in making or planning portions. The term itself does not suggest a specific thing. Perhaps, it is a descriptor that describes portion vehicles that usage electronic frameworks as opposed to cash or checks to coordinate a trade. EFT frameworks are separated into two essential sorts: discount and client. Discount EFT frameworks are frequently used by financial associations for far reaching dollar electronic exchanges. Purchaser EFT frameworks handle an arrangement of electronic portion organizations used by buyers and generally move little dollar entire-ties.

The electronic assets exchange handle should be as protected as could be expected under the circumstances so for this very reason a proposition for a last year venture is presented where the client's security is given the most extreme need. This venture will mean to give a trick verification framework to online cash exchange. Data encryption is used unavoidably as a piece of today's joined society. The two most key elements of bleeding edge data encryption are data insurance and check. As present-day society gets the chance to be more joined, and more information gets the chance to be open there is a necessity for insurances which bring data respectability and data secret.

So, in this last year cash exchange extends, for security, AES calculation is used nearby minute affirmation and consistency check estimation. All these are performed for secure electronic resource exchange. Thus, a customer basically needs to visit any EFT center, with a particular ultimate objective to make the portion. The exchange is done quickly using a single helpful card. Thus, the customer can make the transaction securely as this system uses AES for security and the exchange is being done in a brief moment. At the point when the customer card is separated, it gets a SMS

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 7, July 2021

DOI: 10.17148/IARJSET.2021.8731

message. SMS includes OTP which is fascinating. The customer should simply enter this OTP, which extends level of security. After receiving the OTP, the customer needs to enter the same to perform the desired transaction. This data is being encoded using AES before sending it over the framework. Along these lines, this system ensures security for electronic resource exchange using AES.

This venture means to expel or decrease the absence of encryption. Nonappearance of encryption amidst banks and neighborhood processors show certified perils to the system as transmissions may be blocked and modified or even eradicated. Aggressors may along these lines involve, redirect, or drop stores exchanges. One of the countermeasures is to use open key cryptography to ensure fitting confirmation and insurance taking vulnerability and other required compensating controls to secure cryptographic keys.

OBJECTIVE

The objective of this project is to develop a secure path for transaction done by the user. Using AES (Advance Encryption Standard) the transaction and user account details can be made secured. This system is online so no need of implementation. It can be accessed through internet from anywhere. The system uses AES encryption to encrypt the user account information while transaction. Admin add new area into the system, also add details like ATM Machine ID and Password, ATM caretaker person details.

LITERATURE REVIEW

C. H. Meyer, S. M. Matyas (1981) discussed the personal verification processes at different institutions in an interchange environment are isolated from one another. It is assumed that only information stored on the bank card and information remembered by a sys–tern user is employed for personal verification. It is shown that only through the use of a secret quantity stored on the bank card will the set of required criteria be satisfied. With a personal key, the same degree of isolation can be achieved for authentication of transaction request messages sent from the entry point to the issues.

Dan Zhu (2002) analyzed about modern financial institutions have cashed in on the electronic business opportunities of the Internet by developing numerous payment systems to meet various payment service requirements. In this paper, we examine the function and operation flow of the electronic funds transfer process as well as its security control mechanism. To evaluate telecommunication and data security techniques, a standard leading inter-bank payment system called the Society for Worldwide Inter-bank Financial Telecommunications System is introduced. Some important security features are investigated in detail.

Mintu Philip, Asha Das (2011) Chaotic Encryption Method seems to be much better than traditional encryption methods used today. Chaotic encryption is the new direction of cryptography. It makes use of chaotic system properties such as sensitive to initial condition and loss of information. Many chaos-based encryption methods have been presented and discussed in the last two decades. In order to reach higher performance, these methods take advantage of the more and more complex behavior of chaotic signals.

Mohammed Abudallah MdAysan, Fareed Hassan Almalki, Abdullah Mohammed Almalki (2014) This paper proposes a symmetric key cryptosystem based on the simple mathematical logarithm function. The proposed system benefits from the algebraic properties of log(x) such as non-commutative, high computational speed and high flexibility in selecting keys which make the Discrete Logarithm Problem. Also, the encrypted text converted into binary numbers to make harder to understand by the backer. This method will be suitable in any business house, government sectors, communication network, defense network system, sensor networks etc

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 8, Issue 7, July 2021
DOI: 10.17148/IARJSET.2021.8731

SYSTEM DESIGN

Like in the given Entity relation diagram, the functionality of the program is shown from the user point of view or we can say the tangible working model of the project. The process shows how the different entities are connected to each other and which entity has what job to sincerely perform.

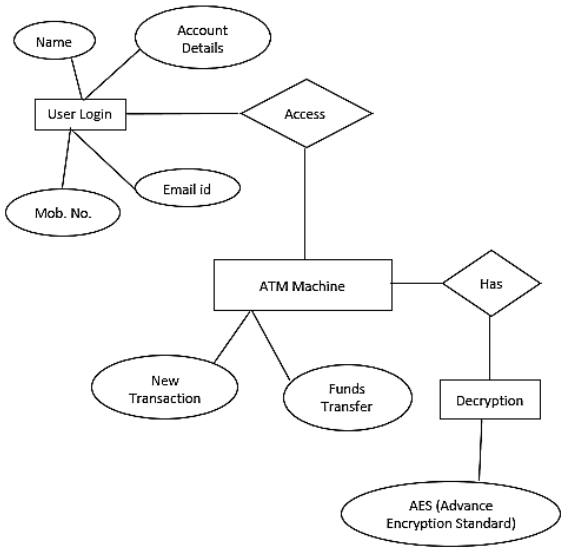

Fig. 1. Entity Relation Diagram

The below 2 flowcharts are the activity flow diagrams for the model, these flow diagrams represent the suggested working design for the project.

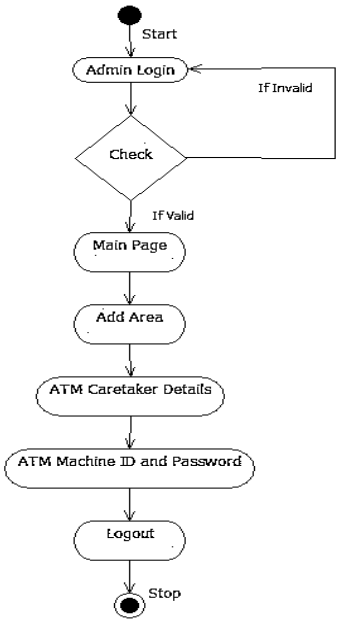

Fig. 2. Admin Activity Diagram

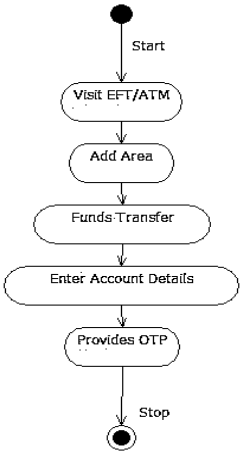

Fig. 3. User Activity Diagram

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 8, Issue 7, July 2021
DOI: 10.17148/IARJSET.2021.8731

Use Case Diagram

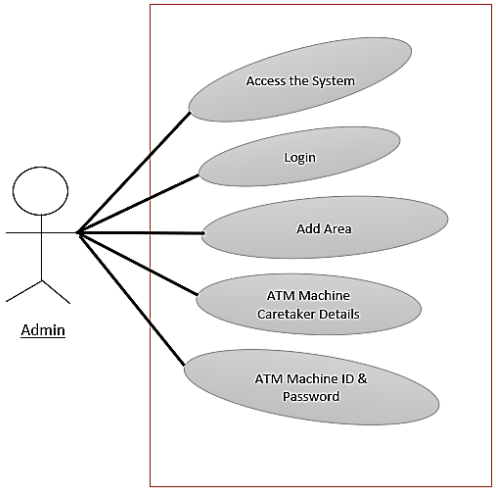

Fig. 4. Admin - Use Case

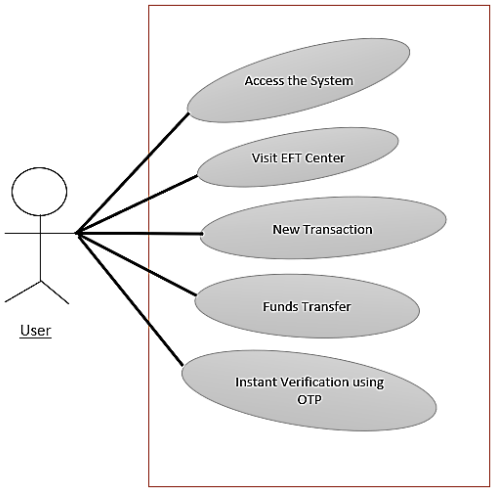

Fig. 5. User – Use Case

AES Algorithm:

AES algorithm works on the BLOCK CIPHER TECHNIQUE; i.e., in this the size of plain text is always equals to the size of cipher key that is being created for the process of both encryption and decryption which makes the process both simpler and more complicated to be cracked.

The AES algorithm consists of multiple rounds of processing of different keys:

- 10 rounds of processing for 128 bits of cipher key.
- 12 rounds of processing for 192 bits of cipher key.
- 14 rounds of processing for 256 bits of cipher key.

The AES algorithm works on the matrix method, as in for the 128-cipher key encryption the model will work with 4 X 4 matrix and creates a matrix using the hexadecimal conversions of each and every character of the input plain text data.

Text	A	E	S	U	S	E	S	A	M	A	T	R	I	X	Z	Z
Hexadecimal	00	04	12	14	12	04	12	00	0C	00	13	11	08	17	19	19

	DEC	HEX		DEC	HEX
A	00	00	N	13	0D
B	01	01	O	14	0E
C	02	02	P	15	0F
D	03	03	Q	16	10
E	04	04	R	17	11
F	05	05	S	18	12
G	06	06	T	19	13
H	07	07	U	20	14
I	08	08	V	21	15
J	09	09	W	22	16
K	10	0A	X	23	17
L	11	0B	Y	24	18
M	12	0C	Z	25	19

Fig. 4. Hexadecimal Conversion Matrix

Implementation of AES Algorithm:

AES defines a 16 x 16 matrix of byte values, called an S-box, that contains a permutation of all possible 256 8-bit values.

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 8, Issue 7, July 2021
DOI: 10.17148/IARJSET.2021.8731

Each individual byte of State is mapped into a new byte in the following way: The leftmost 4 bits of the byte are used as a row value and the rightmost 4 bits are used as a column value. These row and column values serve as indexes into the S-box to select a unique 8-bit output value.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

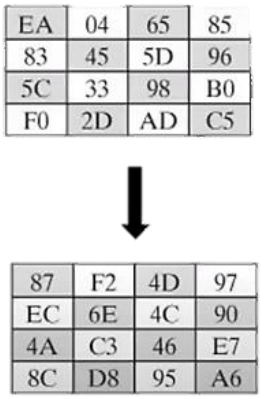

Fig. 5. S-Box

PROPOSED SYSTEM

Nowadays people often need to transfer cash from one account to another. In such cases they need to go to bank or search for PC connected to internet to get access to the services offered by internet banking for reliable fund transfer. This system proves to be really beneficial in such cases. As with the help of this system the user just needs to enter the account details. For security, AES algorithm is used along with instant verification and consistency check algorithm. All these are performed for secure electronic fund transfer.

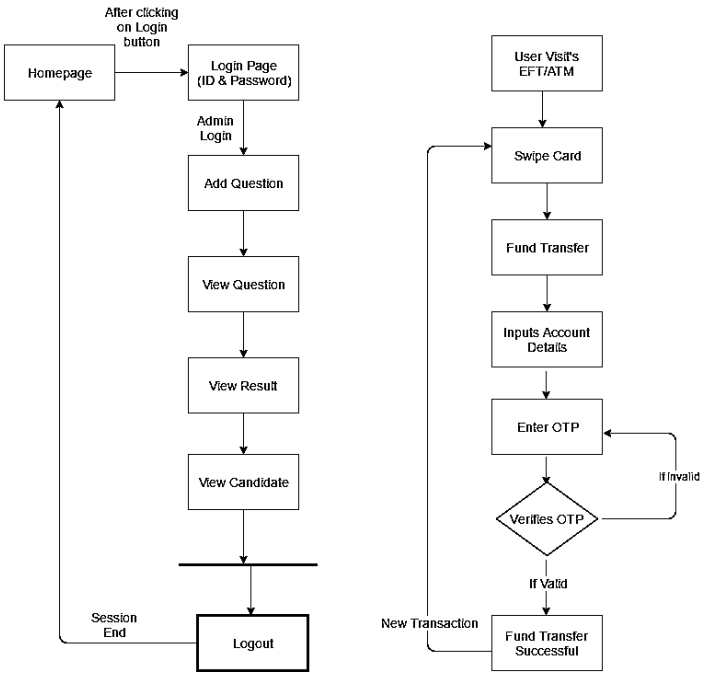

Fig. 5. System Architecture

Thus, a user just needs to visit any EFT center, in order to make the payment. The transfer is done instantly using a single portable card. In this way the user can make the payment securely as this system uses AES for security and the transfer is being done instantly. As soon as the user card is scanned, it receives a SMS message. SMS consists of OTP which is

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 8, Issue 7, July 2021
DOI: 10.17148/IARJSET.2021.8731

unique. All the user needs to do is enter this OTP received which increases level of security. After OTP the user needs to enter account details. This data is being encrypted using AES before sending it over the network. Thus, this system ensures security for electronic fund transfer using AES.

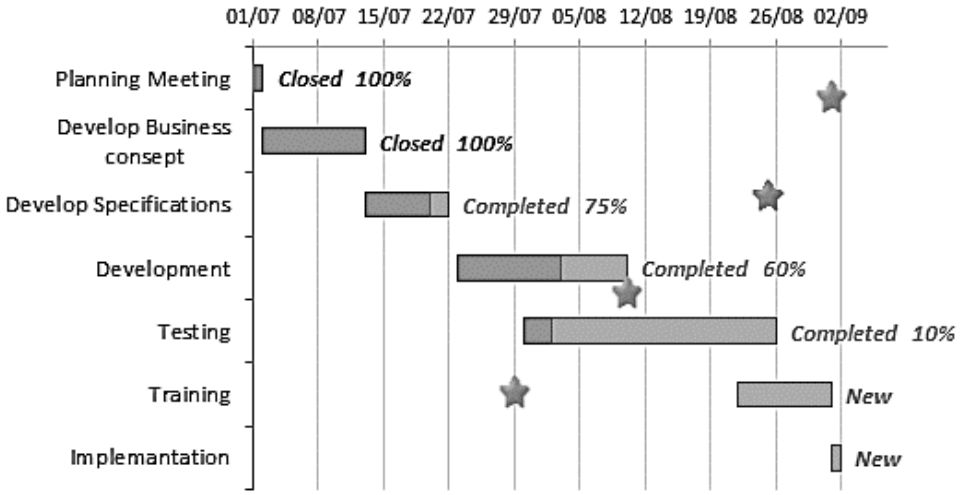

Fig. 6. Gantt Chart

Data Flow Diagram

A Data Flow has only one direction of flow between symbols. It may flow in both directions between a process and a data store to show a read before an update. The later it usually indicated however by two separate arrows since these happen at different type. A join in DFD means that exactly the same data comes from any of two or more different processes data store or sink to a common location. A data flow cannot go directly back to the same process it leads. There must be at least one other process that handles the data flow produce some other data flow returns the original data into the beginning process.

- A Data flow to a data store means update (delete or change).
- A data Flow from a data store means retrieve or use.

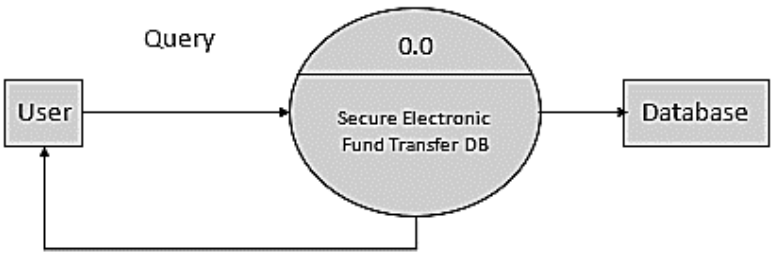

Fig. 6. Database Details Flow Diagram

CONCLUSION

An important point in proposed system is that it demands lesser changes to the present system of Banking and ATM. That means lesser overhead will be required to change the whole system with enhanced security. This project will need to explain to end user, to educate the user to use this system. The main purpose to develop this project is to make a secure path for transaction/fund transfer done by the user. In future work this project can use enhanced and more accurate equipment with better algorithms. More efficient biometric methods can be used like iris scanner, voice recognition etc. Latest algorithms like SHA-3 can be used to generate OTPs.

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 7, July 2021

DOI: 10.17148/IARJSET.2021.8731

REFERENCES

[1]. en.wikipedia.org
[2]. http://msdn2.microsoft.com/en-us/default.aspx
[3]. http://www.asp.net/
[4]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=369803&queryText%3Datm+card
[5]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=824519&queryText%3Datm+card
[6]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6694342&queryText%3Dotp
[7]. C.H.Meyer, S.M.Mat.yas,R.E.Lennon, "Required Cryptographic Authentication criteriafor Electronic Funds Transfer System", CH1629-5/81/089, IEEE, in 1981.
[8]. Dan Zhu, "Security control in Inter-Bank Fund Transfer", Journal of Electronic Commerce Research, VOL. 3, NO. 1, 2002.
[9]. Mohammed AbdallahMdAysan, Fareed Hassan Almalki , Abdullah Mohammed Almalki, "New Symmetric key cryptography algorithm using simple logarithm and binary digits", International Journal of Multidisciplinary Research Academy, Vol.4 issue 6, (in printing) Accepted in March 2014.