International Journal of Engineering & Technology, 7 (2.7) (2018) 993-996

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

Verification of Certificates Using Smart Card Technology

M.V.R.Viswanadh *,M.RameshKumar,T.Chandana

Dept Of Electronics and Computer Science Engineering, KLEF, Vaddeswaram.
**Corresponding author E-mail: viswanadhvamsi2222@gmail.com*

Abstract

Primary aim of current paper is for reducing the certificate duplication and how can we maintain the certificates in a secured form. These two things can be done through a unique certification identification number (UCIN) as a smart card. This card will be validating using the luhn and damm algorithm. To create a paperless atmosphere fraud can also be reduced using the technology of Smart card it decreases certificate maintaining efforts. This technique can also utilize for introducing new technologically in field of Educational by using present trend. with the help of this handling of our documents can be done in an easy manner with that single card.

Keywords: *Authentication complexity, encryption, PIN, UCIN.*

1. Introduction

In general, every organization faces problems regarding fake certificates so this system will provide a solution for this. Here every student will be given a unique number and a card is given. Whenever a student completes his education, his certificates will be entered into his account and whenever an organization needs a certificate[1] it can be accessed easily. So there will not be any chance of fake certificates entering into his account. Through this technique every student from his Secondary schooling level gets a unique certification identification number issued itself by the Secondary board of education, as a Smart card. After completing their secondary education SSC board maintains each student's marks memos with the unique identification in their server database. Likewise, for every higher study students are registered with the same unique certificate identification number and the smart card is credited with all their certificates.
The smart cards are helpful to log on computer even in offline condition also. If the configuration of computers dome for smart card login process then it is helpful for user authenticate when the log on PC by using smart card.

2. Why smart card

2.1 Growing smart cards popularity

Smart cards can be widely used in verity ways around the world. These are very much useful in banking industry like debit cards, Direct TVs also utilized this smart cards for identifying the subscribers as well as the level of subscribers subscriptions in the network of satellite. These cards are used for authenticatio purpose in all fields. With the help this smart card the bank account, satellite dish can be verified for providing the access to the correct persons.

2.2 Help to protect privacy

Storage of the Secure data: The Smart card technology provides data sorting securely on a device or the card. With the help of smart card only, the data can be accessed with appropriate rights for accessing.
Encryption: The technology of the Smart card offers robust encryption capabilities set which also have generation of the key, storage of the secure key[2], hashing as well as digital signing. All the capabilities utilized with the help of system for protecting the privacy in multiple ways.

3. Ease of use

3.1 Smart card enrollment

We must utilize the Smart Card Enrollment Station as well as Certificate Services Web pages for issuing the certificates of the smart card for users. administrators of the Security can issue as well as manage program of the smart card for offering network user high level assurance. When users allowed for requesting its smart card certificate, then the entire security weakens offered by smart cards.

3.2 Personal identification numbers versus passwords

Smart cards advantages are PINs policies may less restrictive compared with network passwords policies. Generally, passwords of good network can be altered regularly as well as having large, composition of the complexity[3]. Because the users may write down its own long, difficult for remembering passwords of the network, network weakened the security. Moreover, good pins

may alter infrequently as well as may short.

4. Process of using smart card

Account number	4	3	8	8	5	7	6	0	1	8	4	x
Double alternate digit	4	6	8	16	5	14	6	0	2	16	4	x
Sum of digits	4	6	8	7	5	5	6	0	2	7	4	x

Fig. 1: Algorithm using LUHN for card validation

Certificates of the Smart card generally requested by CA for authorized agent enrollment. Those one need special certificate to allow for both certificates of the request of the users of other as well as smart cards may given to the authorized persons. The PIN can be settled with the help of smart cards manufacturer. If the user have PIN as well as Smart card then another two things are needed PC which support authentication of smart card as well as reader of smart card[4]. We have to put the card into reader device and entre PIN of that card then log in can be done.

4.1 Requirements

For developing the applications of the smart card, we have some things, those are card reader; A software for communicating to reader and some another software for communicating with smart card which put in reader; as well as smart cards as well as hardware of the smart-card. For communicating to the smart card or for developing the application which requires capable smart-card, should need a reader.
This reader can offered a way to the application for transmitting and receiving commands from smart card. We have different models of readers available in market, those are serial, Card of the PC[5], as well as keyboard models.

5. Algorithm used

Algorithms are used to verify the card numbers if it is valid or not. Describing about the three main algorithms5.1 Model formulation
1. Luhn algorithm
2. Verhoeff algorithm
3. Damm algorithm.

5.1 Luhn algorithm

The algorithm of the Luhn called as "modulus 10"algorithm or algorithm of the "mod 10" , which the easy formula of the checksum utilized for validating a various numbers of the identification, like number of the credit card and IMEI. This type of algorithm used widely. Which designed for a protect for the against of accidental errors, not attacks of malicious. Utmost the credit cards as well as the many government identification no used this type of the algorithm like very much easy method to validate numbers among mistyped or the incorrect numbers.

5.2 Verhoeff algorithm

The algorithm of the verhoeff have the formula of the check sum to detect the error. It may the first decimal checking digit algorithm. It can able to detect all the errors of single-digit as well as errors of the transposition includes 2 digits which are jacent. it utilized the order10 dihedral group properties and combined with the permutation. The algorithm strengths is detecting all errors such as transliteration as well as transposition.

5.3 Damm algorithm

Damm algorithm is like Verhoeff algorithm.It also detecting the all occurred of the most frequently two transcription errors,[6] namely regulating single digit, as well as transport the two digits which are adjacent But the algorithm of Damm has the benefit of making do no need of the the dedicatedly permutations which are constructed as well as specific powers position are inherent in scheme of the Verhoeff .

	LUHN	VERHOEFF	DAMM
Time taken during verification	Faster	Slower	Slower
Length of a card number	Infinite digits(based on issuer)	13-16 digits	Above 10 digits
Works for	All major card	Compared to luhn it is less	Only some cards
Depends on	Last digit	Every number in the card	Every number in the card
Number type	Combination of both digits and chars	Only digits	Only digits
Error detection	accurate	More accurate	accurate
Frequently used alg	More	less	Less
Complexity	O(nkl)	Based on iterations	Based on iterations
Known to	Known to All and usage is more	Known to all usage is less	Known but not used
Who uses	All banks who issues (mastercards,visa,Canadian)	Usage is less	Usage is less

Fig. 2: Comparison of algorithms

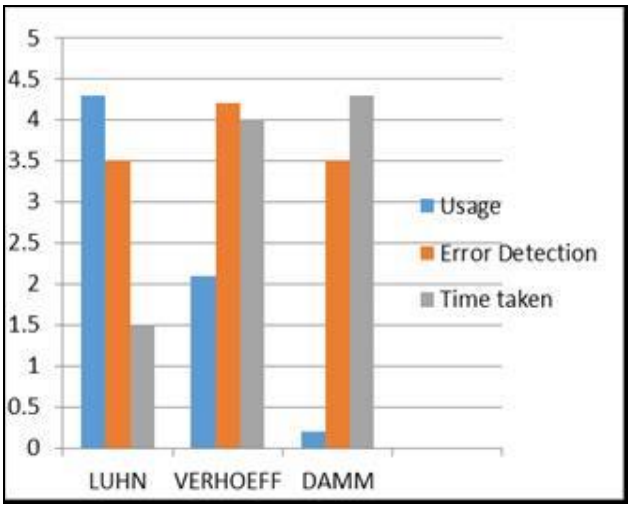

Fig. 3: Bar graph representation for algorithms

Generating the account number of the full. This number may pass with below steps:

1. From digit which is at rightmost, last one can be check digit, that moving the left, 2 digit double the value; when this doubling operation product can be double digit (such as $9 \times 2 = 18$), now the sum digits of products is , 18: $1 + 8 = 9$).

2. Take the sum of all the digits i.e; the obtained digits
When sum total is the modulo 10 can be equal to the 0 ,now this num is can be valid based on Luhn formula; otherwise not valid.
3. Assume an example of an account number "4388576018410707" that will have a check digit added, making it of the form 4388576018410707x:
4. The third row all digits sum is 65+x.
5. The (x) which is check digit can get with the help f of computing non-check digits sum now compute nine times there modulo 10 value.

In algorithm form:

1 .non-check digits Sum (65).
2 .Multiplication dome with 9 (585).
3. product last digit may 5, which check digit. Hence x=5.

Method2: The (x) check digit get with the computation of other digits sum compared to subtraction of unit digit from 10 (65 => Unit digit 5; 10 − 5 = check digit 5).

In the algorithm form:
1. Compute digits sum (65).
2. Consider units digit (5).
3. Subtract unit digit from 10.

Result (5) may be check digit. If the digits sum ends with 0, where the 0 means check digit. It making full account number reading 43885760184107075. Each of the numbers 3885760184107070,43885760184107071, 43885760184107072, 43885760184107073, 43885760184107074, 43885760184107075, 43885760184107076, 43885760184107077, 43885760184107078, 43885760184107079.

If any number we consider as the check digit from above ,they cannot be the exact number for validation of the card number. Only the 5 digit is an exact check digit for the account number.

5.4 Process of Verhoeff algorithm

The Verhoeff algorithm is a formula of the checksum to detect of error develope with Dutch mathematician Jacobus Verhoef in the year 1969. This may1 stalgorithm of the decimal check digit identifies every errors of single-digit as well as all errors of the transposition. Main algorithm strength detecting all errors of the transliteration as well as transposition, Verhoeff algorithm weakness complexity, as well as calculations.

The similar code is like Damm algorithm, that having the usual qualities.

The calculation of the Verhoeff checksum performed like :

1.Creation of the n array out of number individual digits taken from the right to the left
2.From checksum c to the zero Initialization.
3.array n index i, start from zero, replaced the c with the d

The validation of the original number done when the c value is 0. For generating the check digit, 0 insertion done, perform calculation: exact check digit may the inv(c).

5.5 Process of Damm algorithm

Number Validaton oppose to having check digit1. arrange interim digit as well as initialize to the 0.2. number digit Process can be done with digit: Use digit of the number's like column index like s row index, taking table entry along with it.3. validation of number done when result interim digit is 0.

Suppose we choose number (digit sequence) 572.check digit Calculation digit have to processed → column index 572 old digit → row index 097 entryof the table → new digit 974 The 4 is the resulting digit. it calculated the check digit. We insert this to A num as well as obtaining number 5724.number Validating against the check digit is processed → column index 5724 digit which is old → row index 0974 entry of the table → new digit 9740 The result digit is the 0, hence number is valid.

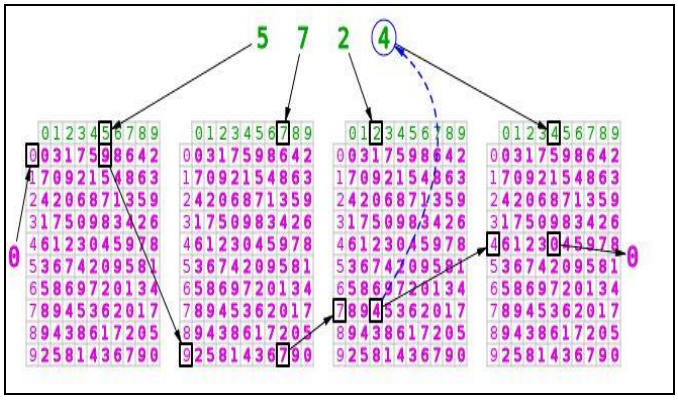

Fig 4: Process determination

When compared to the other algorithms LUHN is better to validate the smart card based on some characteristics these characters are described in below. Based on the characteristics LUHN is better in calculating the checksum, error detection, time taken to validate the smart card, complexity of algorithm, and some other features.

6. Execution results

Luhn algorithm results are displayed as follows:

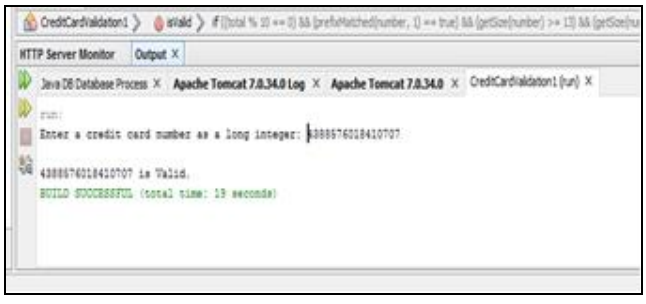

Fig.5: Card number is valid

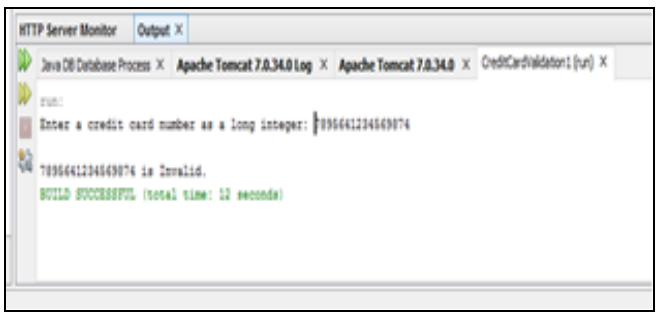

Fig.6: Card number is invalid

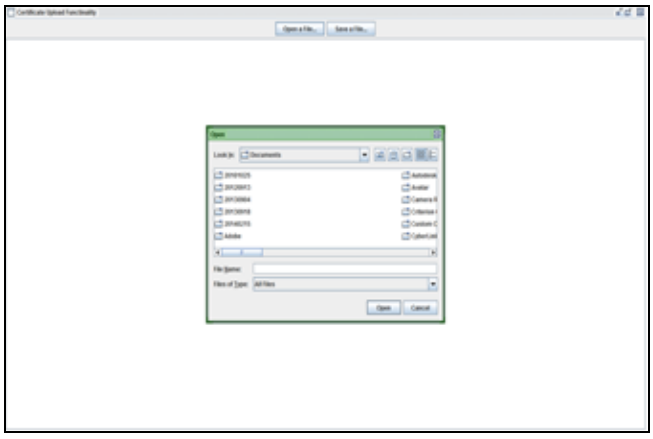

Fig.7: Certificates upload

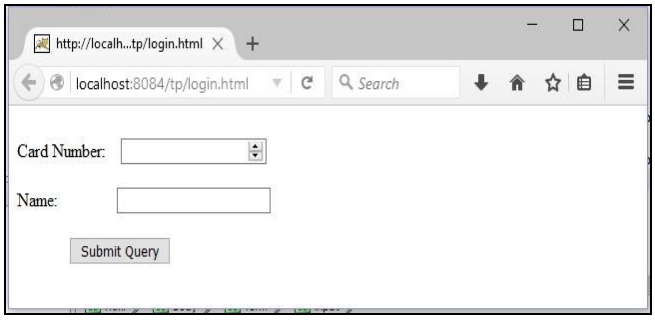

Fig. 8: Login page

7. Conclusion

Many of the smart card systems used in these days serves only one purpose as well as related to the just one another process or is the hardwired to the only one of the application. The smart card may not justifying the existence the respect. The scheme of future of the smart card is towards design of the various application card along own system of operating according to open standard which may be perform functions which are varity in nature.. This can be configurable as well as programmable as well as should be adapted to the new situations as well as various requirements mainly in the areas like security, management of the memory, as well as operating system. All the application methods of the smart card today have the fact that can be code of the functions that can perform ought be importe with operating system from of the card server of the outside. It system weak interms to the security.
Technology of the Smart card, with the ability of identification of the verify as well as the storing as well as the information updated, such as for helping the problems solving well compared to the those industry of the financial services. From the system of the payments perspective,moreover, smart cards have the overcome barriers of several that are unrelated to the technology earlier gaining acceptance of the widespread. barriers may also including higher costs of the product, higher costs of the card-reader, impacts of the uncertain network, a swellas perception where smart card solution of the high-tech in searching of the problem. when all are overcome, like proponents hope, the smart cards may be enable the issuers of the card for precisely market loyalty the related products as well as the services to it's the customers when protect them from the usage of unauthorized card.

References

[1] L.Jagajeevanrao,M.Venkatarao,T.Vijayasaradhi,"journal of Theoritical and Applied information Technology",20th January 2016.
[2] William Stallings, "Cryptography and Network Security Principles and practices", Fourth Edition,November 26,2005.
[3] R. Housley, W. Polk, W. Ford, and D. Solo," Internet X.509 Public Key Infrastructure certificate and certificate revocation list (CRL) profile", RFC 3280, 2002.
[4] P.Urien,M.Badra, and M.Dandjinou,"EAP-TLS smartcards, from dream to reality", 4th IEEE Workshop on Applications and Services in Wireless Networks, Boston, Massachusetts, USA, 2004.
[5] Wen-Fang,Yu,Na,Wang,"Research on Credit Card Fraud Detection Model Based on Distance Sum" ,International Joint Conference on Artificial Intelligence, 2009.
[6] Ashutosh Saxena,Aditya Gaiha,"A Framework for Smart Card-Payment systems".

.