Fuzzy Criptography for Web Data Security

Poli Venkatasubba Reddy

January 13, 2024

Fuzzy Cryptography for Web Data Security

Poli Venkata Subba Reddy
Department of Computer Science and Engineering
College of Engineering
Sri VenkateswaraUniversity
Tirupati, India
vsrpoli@hotmail.com

***Abstract*—Security of the data is major issues for data analytics and data science when the original data is not to be disclosed. The conventional encrypt and decryption methods are not sufficient for security of data particularly web data. There is a fuzzy method useful for not to disclose original data for data analytics of business intelligence. In this paper, data is inherently defied with fuzziness for secrecy. Fuzzy security is studied for web data mining. The data will be fuzzification for data analysis so that the original data need not be disclosed. The fuzzy data mining and fuzzy reasoning is studied for the fuzzy data. Security with encryption and decryption is studied with mind values. Fuzzy Data mining and fuzzy Web data mining is discussed fuzzy sets. The business intelligence is given examples.**

Keywords— fuzzy logic, fuzzy data mining, fuzzy web data mining, fuzzy security, Data analytics

I. INTRODUCTION

Zadeh [13] has introduced fuzzy set as a model to deal with imprecise, inconsistent and inexact, vague and approximate information. The fuzzy set is a class of objects with a continuum of grades of membership.

Fuzzy set A of X is characterized as its membership function A = $\mu_A(x)$ and ranging values in the unit interval [0, 1]

$\mu_A(x)$: X $\rightarrow$[0, 1], x Є X, where X is Universe of discourse.

A = $\mu_A(x_1)/x_1$ + $\mu_A(x_2)/x_2$ + … + $\mu_A(x_n)/x_n$, "+" is union

For instance, the fuzzy proposition "x is best car"

Best car={0.5/Suzuki+0.7/Skoda 0.9/Benz +0.8/Toyota + 0.6/Honda }

The fuzzy logic is as combination of fuzzy sets with logical operators. Some of the logical operations are given below.

Let A, B and C be the fuzzy sets. The operations on fuzzy sets are given as

Negation

If x is not A
$A'=1-\mu_A(x)/x$
Conjunction
x is A and y is B$\rightarrow$ (x, y) is A x B
A x B=min($\mu_A(x)$, $\mu_B(y)$}(x,y)
If x=y
AΛB=min($\mu_A(x)$, $\mu_B(y)$)}/x

Disjunction

x is A or y is B$\rightarrow$ (x, y) is A' x B'
A' x B' =max($\mu_A(x)$, $\mu_B(y)$}(x,y)
If x=y
AVB=max($\mu_A(x)$, $\mu_B(y)$}/x

Implication

if x is A then y is B
A$\rightarrow$B = min{1, 1-$\mu_A(x)$ + $\mu_B(y)$}/(x,y)

Composition

A o R= min $_x$ {$\mu_A(x)$, $\mu_R(y)$}/(x,y), where R=A$\rightarrow$B
A o R==min{$\mu_A(x)$, $\mu_R(x,y)$}/y
If x = y
A o R==min{$\mu_A(x)$, $\mu_R(x)$}/x

Quantifiers

The fuzzy propositions may contain quantifiers like "very", "usually" (concentration) , "more or less" , "unlikely" (diffusion}. These fuzzy quantifiers may be eliminated as

Concentration
$\mu_{very\ A}(x) = \mu_A(x)^2$
Diffusion
$\mu_{more\ or\ less\ A}(x) = \mu_A(x)^{0.5}$

Generalized Constraint

The Generalized Constraint Language[18] is used to deal the fuzzy propositions like "highest sales" for analysis.

For instance,
Item1=0.6
Item2=0.65
"highest sales=max{0.6,0.65}=0.6.

In many cases, the data has to be kept secret for data analytics and data science particularly web data. To keep data security, the data is to be defined with fuzziness inherently. There is a need of fuzzy algorithms and fuzzy data mining algorithms for data analytics and data science.

II. FUZZY DATA MINING ALGORITHMIC LANGUAGE

The fuzzy algorithms[14] are used to solve the fuzzy problems. The fuzzy algorithmic language is discussed for designing efficient fuzzy algorithms for approximate information [14]. The Fuzzy Algorithmic Language is defined as sequence of fuzzy statements.

The fuzzy algorithmic language is to design the fuzzy algorithms for fuzzy problems. The fuzzy algorithm language(FUZZYALGOL) consists of fuzzy variables, fuzzy expressions, fuzzy conditions, and fuzzy loops, etc. These constructs are used for designing fuzzy algorithms for given fuzzy problems.

Here fuzzy algorithms are studied for fuzzy data mining

1. BEGIN initial
   END terminal

2. input fuzzy database output database

read fuzzy database

write fuzzy variables

3. fuzzy statement

Negation

1-A

Union

C = AUB

Intersection

C = A∩B

Association

C = A x B

4. fuzzy inference

If fuzzy condition then fuzzy statement

if x is A_i then y is B_i

5. fuzzy loop

for(i=1;i<=10;i++)

$R_i(x)$=if x_i is A_i then x_i is B_i

6. return fuzzy database

return A

Projection

Proj A = min{$\mu_A(x_1)/x_1$, $\mu_A(x_2)/x_2$, … , $\mu_A(x_n)/x_n$ }

The fuzzy instruction like "go about l00 meters" has to transform into precise form. The fuzzy instructions for " about l00 meters" may be defined as

About l00 meters= { 0.4/80, 0.7/90, 0.9/l00, 0.7/l10 ,0.4/l20}

The minimum grade is selected using the Projection operator for precise instruction.

Proj about l00 meters= { 0.4/l00 }

The execution of fuzzy instruction selects 100 meters with fuzziness 0.9.

Some tomes Center of Gravity(COG) may be used for defuzzification.

Quasi-fuzzy instructions

A Quasi-fuzzy instruction is just machine instruction if a single machine instruction is available[14].

The quasi-fuzzy instruction is fuzzy instruction is defined as

$\mu_A(x) \rightarrow (0 \text{ or } 1)$, where A is quasi-fuzzy set

For instance, "turn right". If turn right" is 1 otherwise 0.

Time complexity

The time complexity for fuzzy algorithm is given by

$\Theta(g(n))$

t_n >=cg(n), where t_n is time taken for input n, c is constant and g(n) is function of n.

For linear fuzzy programming problem, the complexity is given by

programming + projection of fuzzy instructions

$O(n)+O(k)=O(n) \in \Theta(n)$

The fuzzy algorithmic language is necessary to study for fuzzy data mining

1. BEGIN initial

END terminal

2. input fuzzy database output database

3. read fuzzy database

4. write fuzzy variables

5. fuzzy statement

6. fuzzy Negation

1-A

7. Fuzzy Union

C = AUB

8. Fuzzy Intersection

C = A∩B

9. Fuzzy join

$C=A \bowtie B$

$C=A_1 \bowtie A_2 \bowtie \dots \bowtie A_n$

10. Fuzzy decompositions

C=A, B

11. Fuzzy frequency

(t1,f1), (t2,f2), … (tn,fn)

12. Fuzzy clustering

{t1}, {t2}, …, {tm}

13. Fuzzy Association

Ai⇔Bj

14. Projection

15. Proj A = min{$\mu_A(x_1)/x_1$, … , $\mu_A(x_n)/x_n$ }

16. fuzzy inference

17. If fuzzy condition then fuzzy statement

if x is A_i then y is B_i

return fuzzy database

18. return A

III. FUZZY SECURITY FOR DATA MINING

Security methods like encryption and decryption are used cryptography. These security methods are not secured. Fuzzy security method is based on mind and others do not descript. Zadeh [16] discussed about web intelligence, world knowledge and fuzzy logic. The current programming are unable to deal question –answering contain approximate information. For instance " Which is the best car ?". The fuzzy Data Mining with security is knowledge discovery process with data associated.

The Fizzy Relational Databases may be with Fuzzy set theory. Fuzzy Set theory is another approach to approximate information. The security may be provided by approximate Information.

Definition: Given some universe of discourse X, a relational database R1 is defined as pair {t, d}, where t is tuples and d is domains

TABLE I. Relational data base

R1	d_1	d_2	.	d_m
t_1	a_{11}	a_{12}	.	a_{1m}
t_2	a_{21}	a_{22}		A_{2m}
.	.	.	.	.
t_n	a_{1n}	a_{1n}	.	A_{nm}

Definition: Given some universe of discourse X, a fuzzy set is defined as pair {t, $\mu_d(t)$}, where t is tuples and d is domains, and membership function $\mu_d(x)$ taking values on the unit interval[0,1] i.e. $\mu_d(t) \rightarrow [0,1]$, where $t_i \in X$ is tuples .

TABLE II. Fuzzy data set

R1	d_1	d_2	.	d_m	μ
t_1	a_{11}	a_{12}	.	a_{1m}	$\mu_d(t_1)$
t_2	a_{21}	a_{22}		A_{2m}	$\mu_d(t_2)$

.	.	.	.	.	.
t_n	a_{1n}	a_{1n}	.	A_{nm}	$\mu_d(t_n)$

Price = 0.4/50+0.5/60+07/80+0.8/100

The fuzzy security database of Price is given by

TABLE III. Price fuzzy set

ino	Iname	Price
I105	Benz	0.8
I107	Suzuki	0.4
I104	Toyota	0.7
i108	Skoda	0.5
I109	Benz	0.8

Demand=0.4/50+0.5/60+0.7/80+0.8/100

The fuzzy security database of Demand is given by

TABLE IV. Demand fuzzy set

ino	Iname	Demand	μ
I105	Benz	80	0.7
I107	Suzuki	60	0.5
I104	Toyota	100	0.8
I108	Skoda	50	0.4
I109	Benz	80	0.7

The lossless Natural Join of Demand and Price is Union and given by

TABLE V. Lossless join

ino	Iname	Demand	price	μ
I105	Benz	80	100	0.8
I107	Suzuki	60	50	0.5
I104	Toyota	100	80	0.8
I108	Skoda	50	60	0.5
I109	Benz	80	100	0.8

IV. FUZZY SECURITY FOR WEB DATA MINING

The actual data has to be disclosed for analysis on the Web. There is no need to disclose the data if the data is inherently define with fuzziness..

Query language is that queries transforms in to collections of structured and unstructured data for analysis , usually in the form of XML.

A FLWOR expression is constructed from the five clauses after which it is named: FOR, LET, WHERE, ORDER BY, RETURN.

XQuery is to XML DB/XML what SQL is to relational database/tables and XPath is the key to working with XQuery. The structure of an XQuery is called FLWOR (pronounced “flower”). Every XQuery should satisfy the FLWOR structure.

F – For (Optional)
L – Let (Optional)
W – Where (Optional)
O – Ordered By (Optional)
R – Return

Let P is the fuzzy proposition of the query.
P= “Which is the best hardware company?
The answer is “x is the best car”

For instance, the fuzzy set “best car with fuzziness >07” may defined as
For instance,
XML data may be defined as
<CAR>
<COMPANY>
<NAME> Benz <NAME>
<FUZZ> 0.8 <FUZZ>
</COMPANY>
<COMPANY>
<NAME> Suzuki <NAME>
<FUZZ> 0.9<FUZZ>
</COMPANY>
<COMPANY>
<NAME> Toyoto<NAME>
<FUZZ> 0.6<FUZZ>
</COMPANY>
<COMPANY>
I<NAME> Skoda<NAME>
<FUZZ> 0.7<FUZZ>
</COMPANY>

Xquery may define using projection operator for demand car is given as

Name space default = http:\www.automoble.com/company
Validate <CAR> {
For $name in COMPANY/CAR
where $company/ Max($demand>0.7)}
return <COMPANY> {$company/name, $company/fuzzy}</COMPANY>
</CAR>

The fuzzy reasoning may be applied for Fuzzy data Mining.

Consider the more Demand fuzzy database by decomposition.

TABLE VI. Demand

ino	Iname	Demand
I105	Benz	0.8
I107	Suzuki	0.9
I104	Toyota	0.6
I108	Skoda	0.7
I109	Benz	0.9

TABLE VII. Price

ino	Iname	Price
I105	Benz	0.7
I107	Suzuki	0.4
I104	Toyota	0.6
I108	Skoda	0.5
I109	Benz	0.7

The fuzzy reasoning[14] may be performed using Zadeh fuzzy conditional inference

The Zadeh [14] fuzzy conditional inference is given by

if x is P_1 and x is P_2 …. x is P_n then x is Q =

min 1, (1-min($\mu_{P1}(x)$, $\mu_{P2}(x)$, …, $\mu_{Pn}(x)$)) +$\mu_Q(x)$}

The Mamdani [8] fuzzy conditional inference s given by

if x is P_1 and x is P_2 …. x is P_n then x is Q =

min {$\mu_{P1}(x)$, $\mu_{P2}(x)$, …, $\mu_{Pn}(x)$, $\mu_Q(x)$}

The Reddy [12] fuzzy conditional inference s given by

= min($\mu_{P1}(x)$, $\mu_{P2}(x)$, …, $\mu_{Pn}(x)$)

If x is Demand then x is price

x is more demand

----

x is more Demand o (Demand→Price)

x is more Demand o min{1, 1-Demand+Price}Zadeh

x is more Demand o min{Demand, Price} Mamdani

x is more Demand oDemand} Reddy

"If x is more Demand then x is more prices" is given by

TABLE VIII. more demand

ino	Iname	More Demand
I105	Benz	0.89
I107	Suzuki	0.95
I104	Toyota	0.77
I108	Skoda	0.84
I109	Benz	0.95

TABLE IX. Demand→Price

ino	Iname	Zadeh	Mamdani	Reddy
I105	Benz	0.9	0.7	0.7
I107	Suzuki	0.5	0.4	0.4
I104	Toyota	1,0	0.6	0.6
I108	Skoda	0.8	0.5	0.5
I109	Benz	0.8	0.7	0.7

Inference for Price is given by

TABLE X. Inference price

ino	Iname	Zadeh	Mamdani	Reddy
I105	Benz	0.89	0.7	0.7
I107	Suzuki	0.5	0.4	0.4
I104	Toyota	0.77	0.6	0.6
I108	Skoda	0.8	0.5	0.5
I109	Benz	0.8	0.7	0.7

So that the business administrator (DA) can take decision to increase the price or not.."

V. CONCLUSION

Fuzzy Cryptography is encryption and decryption with fuzzification and defuzzification with mind value (fuzzy value). The original data need not be disclosed on web for data analytics. The fuzzy cryptography is discussed for web intelligence.

ACKNOWLEDGMENT

The author thank to iFuzzy2020 Conference Chair for accepting this paper.

REFERENCES

[1] Daniel Sánchez Alvarez and Antonio F. Gómez Skarmeta , "A fuzzy Language", fuzzy Sets and Systems, vol.141, no.3, pp.335-390,2014.

[2] W. Pedrycz and F. Gomide, Introduction to fuzzy Sets, Cambridge, MIT, 1998.

[3] N. Rescher, Many-Valued Logic, McGrow-Hill, New York, 1969.

[4] Sánchez Alvarez Daniel and Antonio F. Gómez Skarmeta , "A fuzzy Language" fuzzy Sets and Systems, vol.141, issue 3, ,pp. 335-390,2014.

[5] E. Santos , " fuzzy algorithms", Information and Control , vol.17, 1970.

[6] H.A. Simon , " The structure of ill structured problems" , Artificial Intelligence , 1973,vol. 4,pp.181-201,1973.

[7] E. H. Mamdani, Application of Fuzzy Logic to Approximate Reasoning Using Linguistic Synthesis, IEEE Transactions on Computers, vol.C-28,issue.2, pp.1182-1191, 1977.

[8] Poli Venkata Subba Reddy Fuzzy data mining and web intelligence, Fuzzy Theory and Its Applications (iFUZZY), 2015 International Conference on, Year: 2015, Pages: 74 – 79

[9] Poli Venkata Subba Reddy, " FUZZYALGOL: Fuzzy Algorithmic Language for Design Fuzzy Algorithms", International Journal of Computer Science and Engineering, 2010,vol.2, issue2,2010.

[10] Poli Venkata Subba Reddy, Fuzzy logic based on Belief and Disbelief membership functions, Fuzzy Information and Engineering, vol. 9, issue 4, pp. 405-422,2018.

[11] . Poli Venkata Subba The proposed "Fuzzy Conditional Inference for Mediiagnosis", Second International Conference on Fuzzy Theory and Technology, Proceedings, Abstract and Summaries of FT&T1993, University of North-Carolina, Duke University, October 13-16, USA,,(1993)193-195.

[12] L.A. Zadeh, "A note on web intelligence, world knowledge and fuzzy logic", Data and Knowledge Engineering, vol.50, pp.291-304,2004.

[13] L. A Zadeh, "Calculus of Fuzzy Restrictions", In Fuzzy Sets and their Applications to Cognitive and Decision Processes, L. A. Zadeh, King-Sun FU, Kokichi Tanaka and Masamich Shimura (Eds.), Academic Press, New York, ,pp.1-40,1975.

[14] L.A.Zadeh , "fuzzy Algorithms" ,Information and Control , vol.12,pp.94-104, 1968.

[15] L.A.Zadeh , "fuzzy Logic" , IEEE Computer , pp.83- 92,1988.

[16] L.A. Zadeh, fuzzy sets, In Control, vol.8,338-353,1965.

[17] L. A. Zadeh, Precipitated Natural Language (PNL), AI Magazine, vol.25, issue 3,pp.74-91,2004.