Implementation of Location Encryption Algorithm for Data Flow in Database Systems Ensuring Enhanced Security Management

Soupayan Datta
Department of Computer Science and Engineering
JIS College of Engineering, Kalyani, West Bengal, India

Soumya Kanta Dey
Department of Computer Science and Engineering
JIS College of Engineering, Kalyani, West Bengal, India

Sudipta Sahana
Department of Computer Science and Engineering
JIS College of Engineering, Kalyani, West Bengal, India

Abstract- In the recent years the storage systems have undergone a rapid transformation with high-end architectural designs being implemented in various storage as well as Business Intelligent Systems. The primary focus has not only been on imbibing mechanisms that provide storage of data at a rapid pace but also adopting security frameworks and protocols so as to secure the vital data stored within these. The recent surge in data storage space requirements has *de facto* contributed to the development of procedures wherein both storage and security could be fused together so as to reduce the complexity that arises while dealing with them separately. This paper with its primary focus on this idea proposes a design wherein the location of data is encrypted along with the data itself using a single Location Encryption Algorithm and can be used in storage segments holding databases. The security has been enhanced further using the Confirmation Code.

Keywords – Location Encryption Algorithm, Main Cipher Text, Small cipher Text, Confirmation Code, Database, Security

I. INTRODUCTION

Considering the demand for storage space over the past century one can only imagine the humongous demand that has to be met in the near future. There has been a consistent effort to develop Business Intelligent Systems which facilitate the same as well as further emphasis on adopting various storage architectures. Those which have been developed has been done keeping in mind the disadvantage that comes with the increase in storage complexity thereby affecting performance primarily downtime. It is pertinent to specify that Data security still remains a challenge that remains to be resolved. Owing to the dynamic nature of the security threats the security frameworks are forced to undergo evolutionary transformations on a frequent basis. It will be justified to say that Security is not a product rather a process.

Our paper has been formulated applying the central concept of using a single algorithm to deal with two main issues – Performance and Security. The overhead that comes with the adoption of a complex architectural design has been considered leading to the formulation of a dual purpose Location Encryption Algorithm. The design has been developed implicitly, but not limited to Storage Segments holding databases. This single yet efficient algorithm presents two benefits. Firstly, it adds to the security of the existing data that can be encrypted using User defined Cryptographic Algorithm. It also makes the retrieval of data easier as the location of the data is present along with the cipher text but in an encrypted form. The security featured presented has been further enhanced by the additional usage of a Confirmation Code which prevents unauthorized access of data to intruders and attackers.

II. RELATED WORK

In M. Bellare [1] formalized the new cryptographic primitive, Message-Locked Encryption (MLE), where the key under which encryption and decryption are accomplished is itself derived from the message. MLE delivers a method to reach secured duplication (space-efficient secure outsourced storage), an objective currently embattled by numerous cloud-storage providers. On the theoretical side the challenge is standard model explanations, and this technique makes.

Chowdhury et al in [2, 3] Symmetric Key encryption was observed to provide a high amount of data privacy and integrity maintain performance and scalability. The security framework that is implemented must be adopted keeping in mind the level of performance since the Database Storage is subsequently used by several users spread over vast geographical locations. A twofold cryptographic algorithmic applying novel procedure for the formulation of the algorithm makes it difficult to decipher and increases the level of security, thereby ensuring authenticated access to the Database Segment.

Bose et al in [4] stated, storage divisions play an essential role in order to achieve the ultimate goal of resource distribution. In addition to the provision of storage division a mechanism has been facilitated so as to search for the required data efficiently (Bose et al., 2015).

Santos et al in [5] proposed the earliest contribution to database design based on algebraic specifications. The paper proposed a formalism adequate for the specification of behavioral properties of data bases. Both update and query requests were modeled in the language of the formal system, and were uniformly treated as a theorem proving process.

II. PROPOSED ALGORITHM

A. Location Encryption Architecture and Data Flow Process-

The flow of data starting from the using raw data and its transformation to cipher text to its storage within the Database Segment can be consolidated using the diagram below-

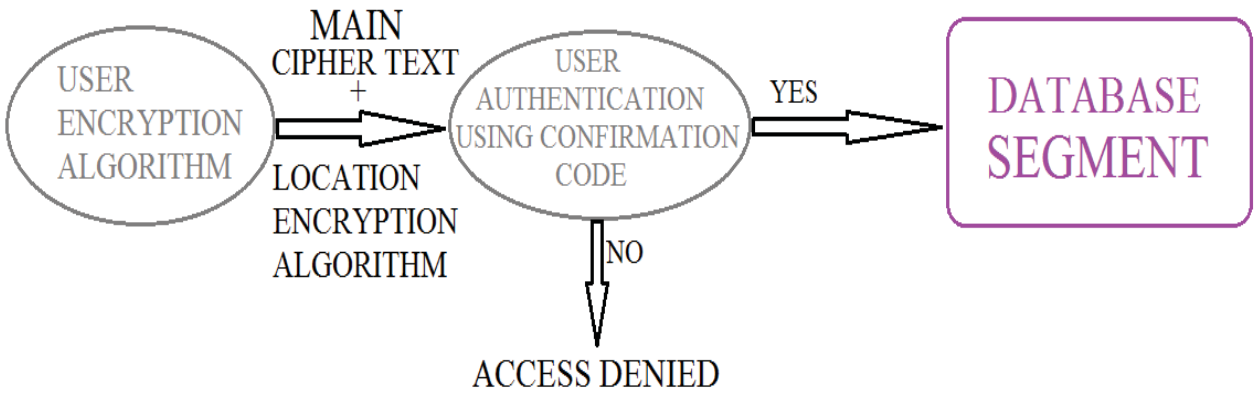

Figure 1. Location Encyption Architectute & Data Flow Design

In order to ensure authorized access of data, a first time user of a storage system adopting this design must register oneself and be authorized to access the Storage Segment. Upon successful completion of first time registration Confirmation Code is generated using the algorithm described later. The generation of the Confirmation Code is based on the Username chosen by the user, and since the Username used by a particular user is unique in every sense, the confirmation Code generated subsequently is also unique.

At its very inception a user defined cryptographic algorithm is used in the generation of the cipher text. Another small cipher text using the Location Encryption Algorithm, mentioned below, is appended to the main Cipher Text obtained using the user defined cryptographic algorithm.

B. Location Encyption Algorithm–

- The small cipher text generated using the Location Encryption Algorithm consists of a 4-digit alphanumeric number. This 4-digit alphanumeric number is appended to the Main Cipher Text obtained using the user defined algorithm. Since the design is developed primarily for databases, keeping in mind this fact every entry in the table(s) can be queried and is present within the Database Segment in its encrypted form.
- The four digits represent the way in which data is stored or the length for which the data has been residing inside the Database.

  a) The first character denotes the specific table/division where the entry is stored. The User has the freedom of choosing the way in which the tables or divisions are created and ordered and the design works perfectly provided the Database does consist of divisions or tables.

  b) The second character denotes the row within a specific table where the queried data is stored.

  c) The third character specifies the file number/column number/data number that needs to be accessed.

  d) The fourth character signifies the year when the data was entered.

The above formulation provides a fast and rapid method in which data can be retrieved within the Database Segment. Moreover the data that are considered redundant owing to its long existence within the system can be deleted just by looking at the last digit of the Small Cipher text.

The Small Cipher Text after being appended to the Main Cipher Text undergoes User Authentication using the Confirmation Code obtained during registration. The Confirmation Code is generated using the steps mentioned below:

C. Confirmation Code-

The generation of Confirmation Code can be explained with the help of an example mentioned below:

- The user chooses an unique Username during the registration process. The username can contain any alphanumeric digit present in the ASCII table including special symbols. “Ak@sh” is considered as the Username.
- The length of the string is 5.

Dec	Hex	Oct	Chr	Dec	Hex	Oct	HTML	Chr	Dec	Hex	Oct	HTML	Chr	Dec	Hex	Oct	HTML	Chr
0	0	000	NULL	32	20	040	&#032;	Space	64	40	100	&#064;	@	96	60	140	&#096;	`
1	1	001	SoH	33	21	041	&#033;	!	65	41	101	&#065;	A	97	61	141	&#097;	a
2	2	002	SoTxt	34	22	042	&#034;	"	66	42	102	&#066;	B	98	62	142	&#098;	b
3	3	003	EoTxt	35	23	043	&#035;	#	67	43	103	&#067;	C	99	63	143	&#099;	c
4	4	004	EoT	36	24	044	&#036;	$	68	44	104	&#068;	D	100	64	144	&#100;	d
5	5	005	Enq	37	25	045	&#037;	%	69	45	105	&#069;	E	101	65	145	&#101;	e
6	6	006	Ack	38	26	046	&#038;	&	70	46	106	&#070;	F	102	66	146	&#102;	f
7	7	007	Bell	39	27	047	&#039;	'	71	47	107	&#071;	G	103	67	147	&#103;	g
8	8	010	Bsp	40	28	050	&#040;	(	72	48	110	&#072;	H	104	68	150	&#104;	h
9	9	011	HTab	41	29	051	&#041;	)	73	49	111	&#073;	I	105	69	151	&#105;	i
10	A	012	LFeed	42	2A	052	&#042;	*	74	4A	112	&#074;	J	106	6A	152	&#106;	j
11	B	013	VTab	43	2B	053	&#043;	+	75	4B	113	&#075;	K	107	6B	153	&#107;	k
12	C	014	FFeed	44	2C	054	&#044;	,	76	4C	114	&#076;	L	108	6C	154	&#108;	l
13	D	015	CR	45	2D	055	&#045;	-	77	4D	115	&#077;	M	109	6D	155	&#109;	m
14	E	016	SOut	46	2E	056	&#046;	.	78	4E	116	&#078;	N	110	6E	156	&#110;	n
15	F	017	SIn	47	2F	057	&#047;	/	79	4F	117	&#079;	O	111	6F	157	&#111;	o
16	10	020	DLE	48	30	060	&#048;	0	80	50	120	&#080;	P	112	70	160	&#112;	p
17	11	021	DC1	49	31	061	&#049;	1	81	51	121	&#081;	Q	113	71	161	&#113;	q
18	12	022	DC2	50	32	062	&#050;	2	82	52	122	&#082;	R	114	72	162	&#114;	r
19	13	023	DC3	51	33	063	&#051;	3	83	53	123	&#083;	S	115	73	163	&#115;	s
20	14	024	DC4	52	34	064	&#052;	4	84	54	124	&#084;	T	116	74	164	&#116;	t
21	15	025	NAck	53	35	065	&#053;	5	85	55	125	&#085;	U	117	75	165	&#117;	u
22	16	026	Syn	54	36	066	&#054;	6	86	56	126	&#086;	V	118	76	166	&#118;	v
23	17	027	EoTB	55	37	067	&#055;	7	87	57	127	&#087;	W	119	77	167	&#119;	w
24	18	030	Can	56	38	070	&#056;	8	88	58	130	&#088;	X	120	78	170	&#120;	x
25	19	031	EoM	57	39	071	&#057;	9	89	59	131	&#089;	Y	121	79	171	&#121;	y
26	1A	032	Sub	58	3A	072	&#058;	:	90	5A	132	&#090;	Z	122	7A	172	&#122;	z
27	1B	033	Esc	59	3B	073	&#059;	;	91	5B	133	&#091;	[	123	7B	173	&#123;	{
28	1C	034	FSep	60	3C	074	&#060;	<	92	5C	134	&#092;	\	124	7C	174	&#124;	|
29	1D	035	GSep	61	3D	075	&#061;	=	93	5D	135	&#093;	]	125	7D	175	&#125;	}
30	1E	036	RSep	62	3E	076	&#062;	>	94	5E	136	&#094;	^	126	7E	176	&#126;	~
31	1F	037	USep	63	3F	077	&#063;	?	95	5F	137	&#095;	_	127	7F	177	&#127;	Delete

charstable.com

Figure 2. ASCII Table

- So, corresponding ASCII code for the username is→ 65 107 64 115 104.

- **4015114670156** is obtained upon reversing the ASCII numbers.

- The length of the string is added to the first digit of the number obtained above. The first number of confirmation code being 4+5=9.. 9 indicates the character i.

- The above sum is then added to the next digit in the number obtained above and the same procedure is followed for all the digits thereby generating the Confirmation Code.
  Now next one should be a alphabet, whose position will be 9+0=9.. Means character will be i .
  Next: a number– 9+1=10; means 1+0= 1
  Next: an alphabet– 10+5=15; means f
  Next: a number– 15+1=16; means 1+6= 7
  Next: an alphabet– 16+1=17; means e
  Next: a number– 17+4=21; means 1+2= 3
  Next: an alphabet– 21+6= 27; means z
  Next: a number– 27+7=34; means 3+4= 7
  Next: an alphabet– 34+0=34; means V
  Next: a number– 34+1=35; means 3+5= 8

Next: an alphabet– 35+5=40; means S
Next: a number– 40+6=46; means 4+6=10, 1+0= 1

The Confirmation code generated for the Username Ak@sh becomes **9i1f7e3z7V8S1**.

IV.CONCLUSION

At a time when Performance and Security is playing an immense role in reference to any storage systems, our proposed design and dual purpose algorithm shall only add to the simplicity with which data is accessed and stored further ensuring the prevention of unauthorized access to data by the attackers. The design comes with the a degree of flexibility since it allows user to adopt his own cryptographic algorithms maintaining the scalable aspect in future , a point that must be considered in development of new technologies in the world of Computer Science.

REFERENCES

[1] Thomas Ristenpart , and Sriram Keelveedhi , Mihir Bellareand, "Message-Locked Encryption and Secure Deduplication", Eurocrypt 2013, Volume 7881, 2013, pp 296-312.

[2] Rajdeep Chowdhury, Soupayan Datta, Saswata Dasgupta, Mallika De, "Implementation of Central Dogma Based Cryptographic Algorithm in Data Warehouse Architecture for Performance Enhancement", International Journal of Advanced Computer Science and Applications, Volume–6, Number–11, November, 2015

[3] Rajdeep Chowdhury, Soumya Kanta Dey, Soupayan Datta, Sweta Shaw, "Design and Implementation of Proposed Drawer Model Based Data Warehouse Architecture Incorporating DNA Translation Cryptographic Algorithm for Security Enhancement", Proceedings of International Conference on Contemporary Computing and Informatics, Pages 55–60, November 2014.

[4] Rajesh Bose, Sudipta Sahana and Debabrata Sarddar, "An Enhanced Storage Management Scheme withSearch Optimization for Cloud Data Center", International Journal of Applied Engineering Research, Volume 10, Number 12, pp. 32141-32150, 2015.

[5] Santos, C. S., Maibaum, T. S. E., and Furtado, A. L. Conceptual modeling of data base operations. nternational Journal of Computer and Information Science vol. 10, pp. 299–314, 1981.