Enhancing Security Privileges to Access SAP-HANA Using UCTD-ABE Scheme

Surajrasal, Kuldeep Prakash
Bharati Vidyapeeth University College of Engineering
Pune, India
surasal@bvucoep.edu.in
kuldeepprakash100@gmail.com

Varsha Rasal
Nehru College of Engineering & Research Centre, Kerala
India
vs.rasal@yahoo.com

Shraddha Shelar
D Y Patil College of Engineering Akurdi, Pune
India
shelartshraddha@gmail.com

ABSTRACT: *SAP HANA is widely used emerging relational database management system. Sensitive data is shared and retrieved through network. Existing cryptographic approach works with security techniques like Attribute Based Encryption, Cipher Text, Decentralized Approach, & Mediator approach. Multiple approaches enhances the security level but in dept individual approaches keens to enhance security level. In proposed approach, UCTD-ABE scheme is applied where User, Current data, Time and Date attributes are used to enhance the existing approach of Attribute Based Encryption. In proposed concept, all attributes are used based on situation. Accordingly logic will be applied. This situation based attribute selection and applied logics enhances the security approach in SAP HANA.*

Keywords: ABE (Attribute Based Encryption), A_E (Encrypted data), U_A (User Attribute), C_D (Current data Attribute), T_A (Time Attribute), D_A (Day Attribute), SAP, SAP-HANA

Received: 13 January 2017, Revised 1 March 2017, Accepted 5 March 2017

1. Introduction

The business market and strategies keep changing rapidly. Hence, a company needs to have a fast and effective use of data and information in order to respond quickly to the changes and requirements. Therefore, a need for a modern high performance platform felt which could process huge amount of real time data efficiently for analytic and business applications. System Application Product High Performance Analytic (SAP HANA) fulfils the requirements of the modern business world. SAP

HANA is a combination of HANA database, data modeling, HANA administration and data provisioning in a single suite [1]. Traditional software are dependent on the layers of information which are present at the different levels of details and are to be presented in a correct format whereas SAP HANA is dependent on one copy of information which is stored once and is calculated when there is a demand for response. SAP HANA is an in-memory platform which means that all the data from source system is stored in a RAM due to which there is no wastage of time in loading data from hard disk to RAM [2]. It combines the ACID compliant database with the advanced data processing, application services and flexible data integrity services and can also act as a SQL based relational data base. In SAP business Warehouse (SAP BW), SAP Business Suite (SAP BS) or S/4 HANA [3].

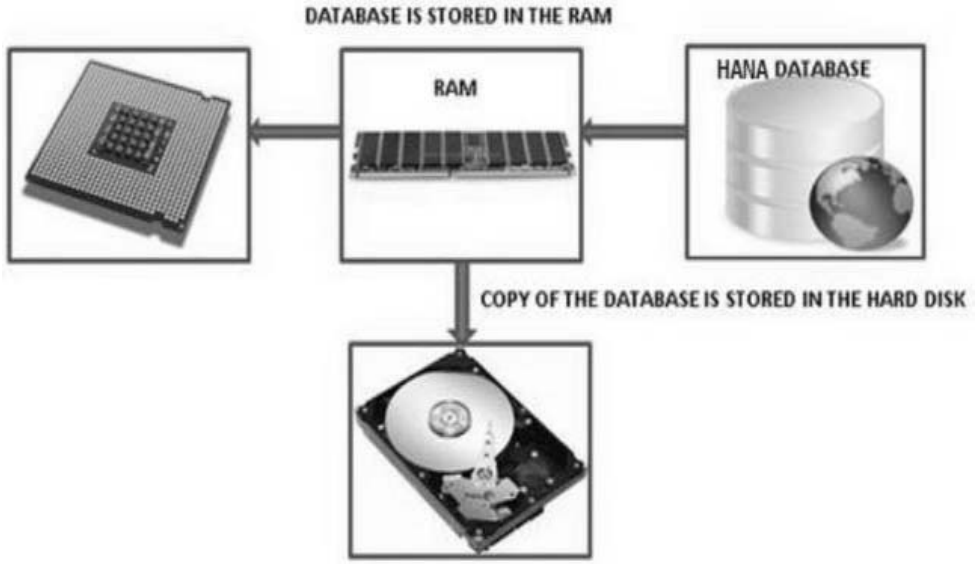

Figure 1. SAP HANA in-memory database [1]

The in-memory real time operational analytics of SAP HANA gives flexible analysis of operations on detail levels providing primary persistence layer and optimization for complete business suites, OLAP, OLTP and SAP BW. There are various deployment options available like on premise, host, public or managed cloud for quicker adaptation, instant availability and reduce cost [4]. It provides its customers a remarkable query performance for enhanced decision making on a common modeling environment with seamless usage of data and reusable services to manage analyze the data along with security and ease of maintenance.

2. Existing Security Architecture

SAP HANA has been introduced as a solution to the uprising issues regarding the secure transaction and safe data storage. For an organization it is a matter of great concern to keep the critical data protected from unauthorized access and follow the rules and regulations according to the standards established. This has resulted into making databases and technology stack as the treasure of the organization and the information security as the primary task in business world [5].

Prevention	Detection
Authentication & Authorization	**Data Discovery & Classification**
Database Firewall	**Privilege Analysis**
Encryption	**Configuration Management**
Data Reduction & Masking	**Audit Logging**
Patch management	

Figure 2. Security objectives [2]

2.1 Security Architecture

SAP HANA supports multitenant database containers which are multiple databases in a single HANA system. A HANA system can have several multitenant database containers but only one system database. A SAP HANA system which is installed in such environment is identified by a single system ID (SID) and the database containers are identified by a SID and database name [2]. The administration clients which access the database using SAP HANA HDBSQL or SAP HANA studio connects to specific databases. SAP HANA provides user and role management. For Authentication the database is used to authenticate the clients using SQL interface and the HTTP clients that connect to SAP HANA XS. Authentication methods used for integration of HTTP access through SAP HANA XS into SSO environment are SAML, X.509 client certificates, Kerberos with Simple and Protected GSSAPI Negotiation Mechanism (SPNEGO), and SAP logon/assertion tickets.

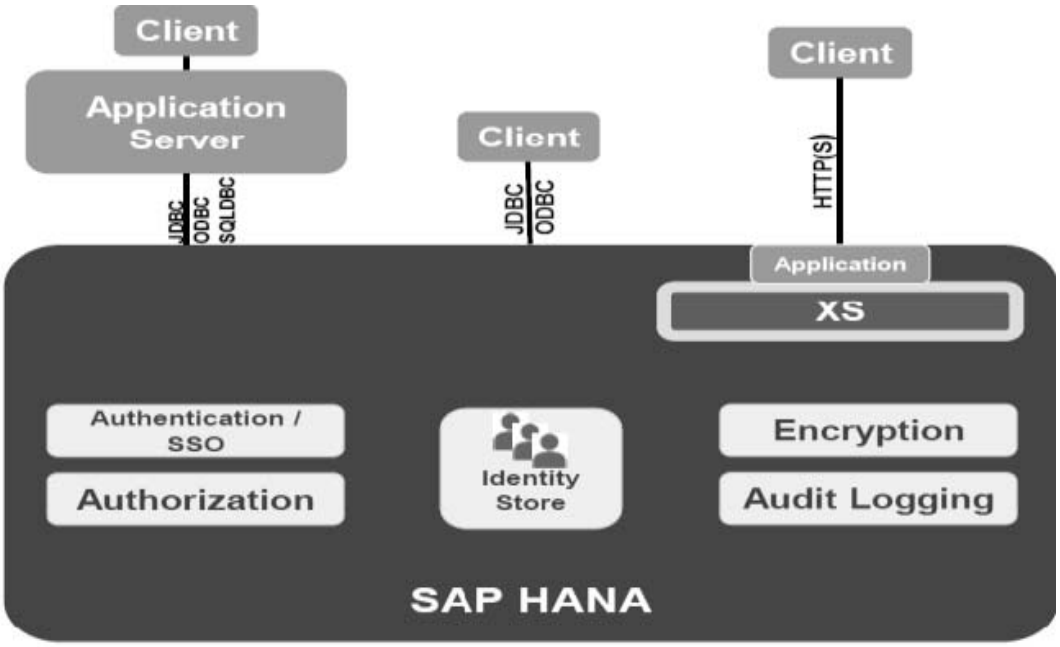

Figure 3. SAP HANA Security Architecture [3]

Using SAP HANA as a database does not change the security features provided by the traditional security architecture such as Authentication, Authorization, Encryption and Auditing. Along with these, it includes some additional features such as Database Isolation, Configuration Change blacklist and Restricted Features [8]. Database Isolation involves prevention of cross tenant attacks through operating system mechanism. Configuration Change blacklist involves prevention of certain system properties from being changed by tenant database administrators. Restricted Features involves disabling certain database features that provides direct access to file system, the network or other resources [7].

For logon, users must exist in the Identity Store of the SAP HANA database. Privileges are granted to the database users for the Authorization to access the applications and functions. To secure the communication between SAP HANA XS server and HTTP client Encryption of data communication in the network Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are supported and recommended for network communication where possible. The SAP Web Dispatcher which manages the incoming HTTP requests is configured in order secure communications between SAP HANA system and HTTP clients. Encryption of data persistence layer is performed in order hide the actual data from anyone that accesses the data volume on disk using operating system commands. Auditing is possible for all the actions performed in the SAP HANA database [6].

2.2 Security Functions

2.2.1 Applications

It is the end users clients that are accessing the database through SQL interface and the HTTP clients connecting to the server. The application server and SAP HANA XS are present for the user administration and role management for secure access and communication [3].

2.2.2 Tools

The main administration and monitoring tool for SAP HANA is SAP HANA Studio used for maintaining the runtime security configuration, manage users, role management, and authorization, monitoring security and configuring audit logging [3]. In addition to it, other tools available are SAP HANA Web IDE, SAP HANA Cockpit and HDBSQL.

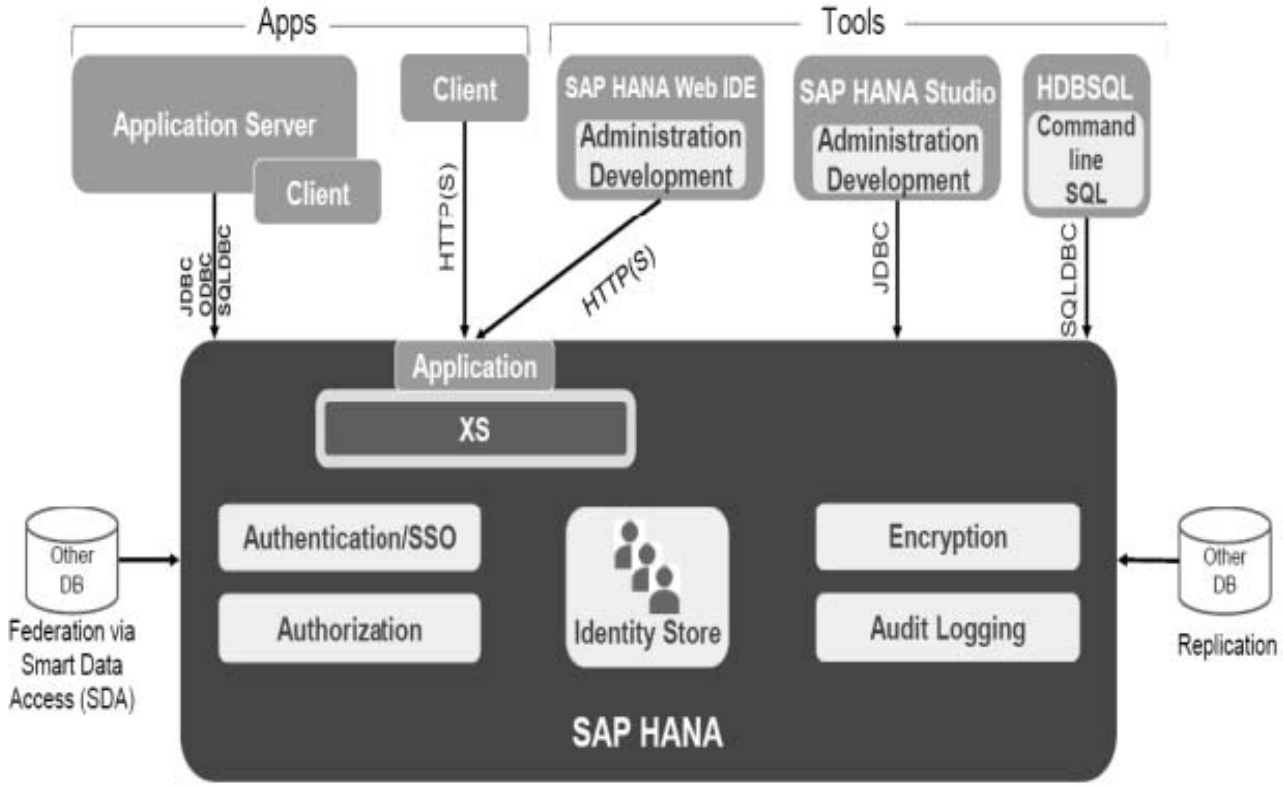

Figure 4. Overview of security functions [3]

2.2.3 Connectivity

SAP HANA provides mainly two types of Connectivity-

HTTP/HTTPS:

- User name and Password
- Kerberos via SPNEGO
- SAML
- SAP logon assertion tickets
- X.509

JDBC/ODBC/SQLDBC:

- User name and Password
- Kerberos
- SAML
- SAP logon assertion tickets

2.2.4 Functions

SAP HANA architecture has designed its segments based on functionality [3].

1) User and Role Management

SAP HANA has database administrators, technical database user or administration clients as the users accessing the database according to the given scenario. SAP HANA tools are used for user administration and role assignment. To order to integrate to the existing user provisioning infrastructure, SAP Identity Management and GRC Access Control are use for which adaptors are available. SQL interfaces are used to connect to the custom user provision solution.

Roles are used to bundle and structure privileges and can be assigned to users. Developers design the roles which are stored in the repository. The roles are exported to the production system for activation and to be run by the users.

2) Authentication

In order to access SAP HANA data, functions and application, authentications is required. It allows control over the user access and security. Various authentication mechanisms are used depend on the scenarios. It is facilitated by the two connectivity protocol, HTTP/HTTPS and JDBC/ODBC/SQLDBC where HTTP/HTTPS are managed by the Internet Connection Manager (ICM). There is no default password option available due to which users are forced to set password. There are several single sign-on options are available such as Kerberos/SPNEGO, SAML, SAP logon and assertion tickets, X.509.

3) Authorization

Authorization is the mechanism used in SAPHANA to ensure that authenticated users can perform only those things they are allowed to do. It also specifies which user is allowed to access which data and for which activities.

The actions that a user can perform depend on the assigned roles and privileges. Roles are used to bundle and structure privileges, allowing to create sets of privileges for dedicated user groups. Technical database users and data base administrators with necessary authorization can modify roles and create customized roles. Users are authorized to execute a procedure, function or a system activity by granting privileges to them either directly or through roles. The types of privileges available in SAP HANA database are:

• **System Privileges:** Involve authorizing general system-level operations and administrative tasks and those for SAP HANA repository authorizes users to perform basic repository operations.

• **Object Privileges:** Involve authorizing specified actions on specified database objects.

• **Analytic Privileges:** Involve authorizing selective access to data in SAP HANA information models which has analytic views, attribute views, and calculation views.

• **Package Privileges:** Involve authorizing package operations.

• **Application Privileges:** Involve authorizing access to applications while configuring which data has to be exposed and setting rules for exposing URLs

4) Identity Store

Identity store is the part of SAP HANA where the users are stored for the database. For logon, the user must exist in the identity store.

5) Encryption

Secure configurations come with SAP HANA as default which allows customizing the system according to the implementation and system environment. Some settings are significantly essential that any miss configuration in them may the leave system in vulnerable state.

Encryption as a bypass of authorization on the lower layers of architecture and is the primary method for fine granular access

control. Encryption of data persistence layer is performed in order hide the actual data from anyone that accesses the data volume on disk using operating system commands. Data at rest is encrypted and stored as persistent storage in order to provide a recovery from failure. XS applications are provided with the encryption APIs and there are several third party backup tools available for advanced backup encryption and key management capabilities.

6) Audit Logging

Auditing is possible for all the actions performed in the SAP HANA database. Audit logging records critical system events. The Data recorded to it are such as changes to roles and users or the database configuration. The read and write access to objects and execution of procedures can also be recorded. Both successful and unsuccessful actions can be recorded. Firefighter logging is enabled when a higher privileged user requires temporary access to a critical system in order to track all the actions of a specific user. These recorded events are either written into the Linux syslog or a secure database table within SAP HANA.

3. Research Methodology

Encryption decryption techniques are applied on both ends, at SAP HANA basement & client [3].While delivering sensitive data over internet, it keens to improve its security because of unsecured. Different types of protocols, techniques are used and supportive like http, Java, SQL but techniques are not as that much secured [4]. Even though SAP HANA basement has designed with encryption techniques and administrative tools, it keens to improve its security level to access valuable database. Based on existing approach, proposed approach is designed to make it more secure. Actual data needs to be hiding to enhance security. Attributes are assumed to make database more secure [12], [15].

3.1 Configuration and Synchronization Of SAP HANA Secured Application Layer

SAP HANA runs on platform which has to be installed on client as well as server side. Its application platform is important segment to use SAP HANA service. Major requirement is internet connection. In the first attempt of registration, all logical and segmental will be synchronized at the server side.

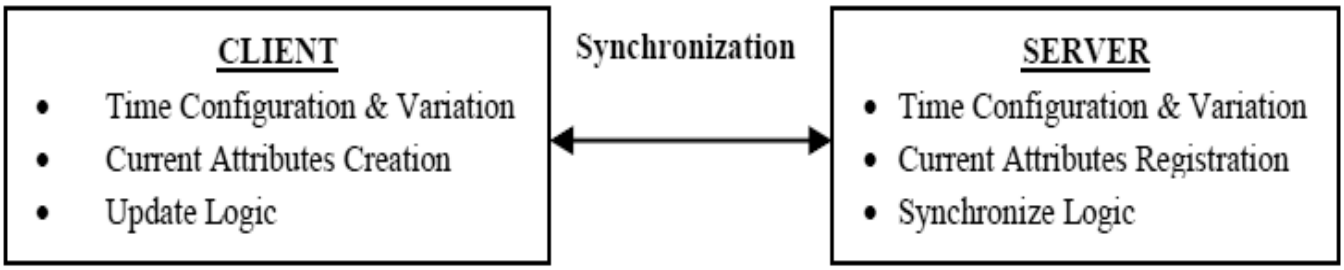

Figure 5. First time SAP HANA secured application layer configuration and synchronization

SAP HANA security architecture has some segments like Encryption, Audit login, Identity store, Authentication, Authorization, Apps and tools [3], [6]. In proposed approach, existing encryption segment is replaced with UCTD (User Current data Time Date) - ABE (Attribute Based Encryption) system. Proposed approach denotes own and some referenced logic to make secure communication while using SAP HANA.

1) Time Configuration & Variation

Client and server time may vary due to difference in locality or other reasons. While installing application platform on client side, system time is stored on server side. While installation there is possibility of time variation (TV). Time variation is the difference in time between client system and server system. Difference is considered in terms of hours: minutes. According to difference in time, client details are registered on server side.

2) Current attributes Creation & registration

In SAP HANA ERP (Enterprise Resource Planning) model, client requirements are gathered and based on these requirements.

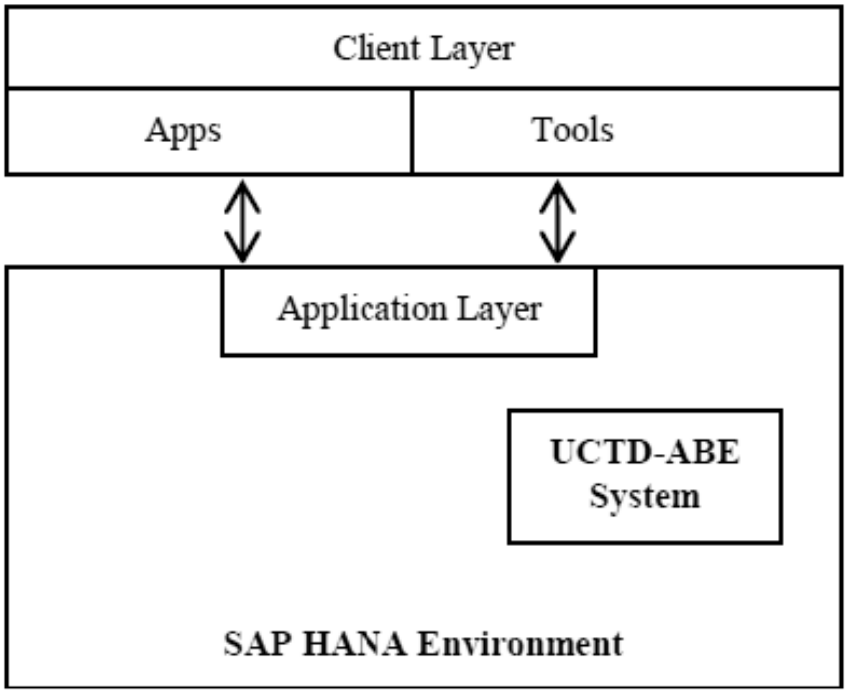

Figure 6. UCTD-ABE system with SAP HANA

Options are created in user interface. Current attributes are allocated according to these options available. These created current attributes at the client side are simultaneously stored on server side.

3) Updating logic & Synchronization

After completion of all steps including configuration and attributes creation, all major components in SAP HANA application platform are synchronized between client and server, after which client is officially registered at server including secured server application platform.

3.2 Logical and Mathematical Approach

Logical approach is applied to select and process attributes based on user activities and selection. Random logics are applied based on user actions. Mathematical approach is applied to form encrypted data and security based calculations.

3.2.1 Attributes Creation

Attributes are allocated and used in computing so that original data can be securely stored and hide [11].

Attributes are allocated to respective component details to store them with secured and safe medium. Main attribute sets are User attribute (U_A), Current data attribute (C_D), Time attribute (T_A) and date attribute (D_A). Accordingly sub attribute sets are created [12].

a) User Attributes

User attributes are assigned instead of directly using user details while doing transactions and computation. In the earlier cryptographic approaches user attributes are considered as most secured assumed elements to hide user details [9], [10]. User details may include elements like 'name', 'sirname', 'city', 'pincode', 'mobile number' & 'date of birth' [12,16]. It can be represented in the set format. Attribute set is considered as U_A

$$U_A = \{\text{'name', 'sirname', 'city', 'pincode', 'mobile number', 'date of birth',}\ldots\ldots\}$$

In proposed approach, attributes are allocated for respective user details which are indirectly components of user details.

U_A= { 'u_1', 'u_2', 'u_3','u_4', ……., 'u_n'}

b) Current Data Attributes

In SAP HANA, user selects options as per requirement. According to user option selection, attribute will be assigned randomly based on logic. These available options are already synchronized with SAP HANA server while doing first configuration setup at client side. Current data attribute set is considered as C_D and its elements are d_n

C_D = {'*Option*1', '*Option* 2', '*Option* 3',……, '*Option n*'}

C_D ={' *o*1', '*o*2', '*o*3', '*o*4',…..., ' *on*'}

c) Time Attribute

System time has twelve hours and sixty minutes. Hour and Minute attribute sets are considered. Hour attribute set has twelve elements (T_{A1}) and Minute attribute set (T_{A2}) has sixty elements. Main time attribute set is considered as T_A. Based on system time and logic, attribute set elements will be used.

T_{A1} = {'1', '2', '3', '4',…...,'12'}

T_{A1} = {'t_1', 't_2', 't_3', 't_4',….., 't_{12}'}

T_{A2} = {'1','2', '3', '4',…...,'60'}

T_{A2} = {'ta_1', 'ta_2', 'ta_3', 'ta_4',….., 'ta_{60}'}

T_A= {t_n, t_{an}}

d) Date Attributes

System date format is considered as date/month/year format. Date attribute set (D_A), Date (D), month (M) and day (D_y) are considered. Date attribute set has thirty one elements, month attribute set has twelve & day attribute set has seven elements.

D = {'1','2','3',…...,'31'}

D = {'d_1', 'd_2', 'd_3', 'd_4', 'd_5',…...,'$\boldsymbol{d}_{31}$'}

M = {'*January*', '*February*', '*March*', '*April*',……., '*December*'}

M = {'m_1','m_2','m_3',….., 'm_{12}'}

D_y = {'*Monday*', '*Tuesday*', '*Wednesday*', '*Thursday*',….., '*Sunday*'}

D_y = {'d_{y1}', 'd_{y2}', 'd_{y3}', 'd_{y4}',….., 'd_{y7}'}

D_A = {d_n, m_n, d_{yn}}

D_A set includes selected elements from D, M & D_y based on situation.

3.2.2 Logical Approach

Only registered attributes are considered as a valid valued attributes. Attributes are selected based on logic applied on attribute set. Logics are created based on requirement and conditions.

a) Time Attribute Selection Logic

Time attributes is allocated according to systems timing. At the time of communication, if system time is *HH:MM:SS* means *HH* hours, *MM* minutes and *SS* seconds, attributes allocated are

$$t_n = HH$$

$$t_{an} = MM$$

where *HH* and *MM* are respective values. Here attribute set will have single element which is selected from Time attribute set.

$$T_{A1} = \{t_n\}$$

$$T_{A2} = \{t_{an}\}$$

b) User & Current Data Attribute Selection Logic

Attribute will be selected based on the condition and situation during user's communication. Five sub logics l_1, l_2, l_3, l_4 & l_5 are considered for user & current data attribute element selection. U_A and C_D elements are picked up from stored attribute sets based on logic. These selected elements are added to the required attribute sets which are used in encryption. Day divisions are considered as Morning (M_R), Afternoon (A_F), Evening (E_V), Night (N_G) & Midnight (M_G). Accordingly, attribute selection logic will be applied.

Logic	Day Division	Time Session condition	Applied Description
l_1	M_R	IF $6 \le t_n$(Value)<12	Elements are selected from stored U_A & C_D attribute sets in even sequential order respectively.
l_2	A_F	IF $12 \le t_n$(Value)<4	Elements are selected from stored U_A & C_D attribute sets in odd sequential order respectively.
l_3	E_V	IF $4 \le t_n$(Value)<9	Elements are selected from stored U_A & C_D attribute sets in reverse order of M_R respectively.
l_4	N_G	IF $9 \le t_n$(Value)<2	Elements are selected from stored U_A & C_D attribute sets in reverse order of A_F respectively.
l_5	M_G	IF $2 \le t_n$(Value)<6	Elements are selected from stored U_A & C_D attribute sets in first half according to M_R and remaining half according to A_F respectively.

Table 1. Attribute sets element selection logic for U_A & C_D

c) Main Attribute Set Formation Logic

In approach, main attribute sets are considered as U_A, C_D, T_A & D_A. On hourly basis, logic gets changed and applied. Term hourly basis refers to the twelve hour clock. According to respective hours, logics are applied to on attribute sets to select and to form main attribute set. Here main attribute set is considered as A. A is main attribute set which is union of all considered attribute set elements with respect to applied logic [12]. D_S is data size in kilo bytes (*KB*). For even and odd identification, data size is considered.

$$A = U_A \, U \, C_D \, U \, T_A \, U \, D_A$$

Here to apply sequential order logic new attributes are considered based on which logic will be applied to form main attribute set.

$$U_A \rightarrow_{A1}, C_D \rightarrow_{A2}, T_A \rightarrow A_3, D_A \rightarrow A_4$$

Main attribute set elements are arranged in logical sequence according to situation and condition.

Logic	**Condition 1 (Con_1)**	**Condition 2 (Con_2)**	**Applied Description**
L_1	IF t_n(Value)=1	D_S= Even	**IF (Con_1) AND (Con_2) Attribute set sequence is A_1, A_2, A_3, A_4 IF (Con_1) reverse the sequence**
L_2	IF t_n(Value)=2	D_S= Odd	**IF (Con_1) AND (Con_2) Attribute set sequence is A_1, A3, IF A_2, A_4 (Con_1) reverse the sequence**
L_3	IF t_n(Value)=3	t_{an}(Value)= Even	**IF (Con_1) AND (Con_2) Attribute set sequence is A_4, A_1, A_2, A_3 IF (Con_1) reverse the sequence**
L_4	IF t_n(Value)=4	t_{an}(Value)= Odd	**IF (Con_1) AND (Con_2) Attribute set sequence is A_1, A_2, A_4, A_3 IF (Con_1) reverse the sequence**
L_5	IF t_n(Value)=5	t_n(Value)* t_{an}(Value)= Even	**IF (Con_1) AND (Con_2) Attribute set sequence is A_1, A_1, A_2, A_2, A_3, A_3, A_4, A_4 IF (Con_1) reverse the sequence**
L_6	IF tn(Value)=6	t_n(Value)* t_{an}(Value)= Odd	**IF (Con_1) AND (Con_2) Attribute set sequence is A_1, A_2, A_3,A_4,A_1,A_2,A_3,A_4 IF (Con_1) reverse the sequence**
L_7	IF tn(Value)=7	t_n(Value)mod t_{an}(Value)= Even	**IF (Con_1) AND (Con_2) Attribute set sequence is A_1, A_2, A_1,A_2, A_3, A_4, A_3, A_4 IF (Con_1) reverse the sequence**
L_8	IF tn(Value)=8	t_n(Value)mod t_{an}(Value)= Odd	**IF (Con_1) AND (Con_2) Attribute set sequence is A_1, A_2, A_3, A_3, A_2, A_1,A_4 IF (Con1) reverse the sequence**
L_9	IF t_n(Value)=9	t_n(Value)mod t_{an}(Value)= 0	**IF (Con_1) AND (Con_2) Attribute set sequence is A_1, A_2, A_2,A_3, A_3,A_4, A_4, A1 IF (Con_1) reverse the sequence**
L_{10}	IF t_n(Value)=10	t_{an}(Value)mod t_n(Value)= Even	**IF (Con_1) AND (Con_2) Attribute set sequence is A_1, A_3, A_2, A_4, A_1,A_3, A_2, A_4 , A_1, A_3, A_2, A_4. IF (Con_1) reverse the sequence**
L_{11}	IF t_n(Value)=11	t_{an}(Value)mod t_n(Value)= Odd	**IF (Con_1) AND (Con_2) Attribute set sequence is A_4, A_3, A_2, A_1,A_1,A_2, A_3, A_4, A_2, A_4, A_1, A_3 IF (Con_1) reverse the sequence**
L_{12}	IF t_n(Value)=12	t_{an}(Value)mod t_n(Value)= Odd	**IF (Con_1) AND (Con_2) Attribute set sequence is A_1, A_1, A_1, A_2,A_2,A_2,A_3, A_3, A_3, A_4, A_4, A_4 IF (Con_1) reverse the sequence**

Table 2. Main Attribute set elements selection logic

3.2.3 Attributes Assembly

Attribute set formed is applied further for encryption. For decryption, its elements and their selection logic is important. While synchronization process, time variations will be noted and accordingly rest of the computing will be done.

If client is accessing SAP HANA server on 15th August, Monday in 2016 year at 5.30pm, '5' is t_a and '30' is tan which is even. Based on situation, logic 'l_3' from Table. I and 'L_5' from Table. II are applied.

$$\text{IF } 4 \le t_n(\text{Value}) < 9$$

$$U_A = \boldsymbol{A_1} = \{u_{n+2}, \ldots, u_6, u_4, u_2\}$$

$$C_D = \boldsymbol{A_2} = \{o_{n+2}, \ldots, o_6, o_4, o_2\}$$

$$T_A = \{\text{'5'}, \text{'30'}\} = \boldsymbol{A_3} = \{t_n, t_{an}\}$$

$$D_A = \{\{\text{'15'}, \textit{'August'}, \textit{'Monday'}\} = \boldsymbol{A_4} = \{d_{15}, m_8, d_1\}$$

$$A = U_A \, U \, C_D \, U \, T_A \, U \, D_A$$

IF $t_n(Value) = 5$ & $t_a(Value)$* $t_{an}(Value)$= *Even apply sequence as* $A_1, A_1, A_2, A_2, A_3, A_3, A_4, A_4$

$$A = \{u_{n+2}, \ldots, u_6, u_4, u_2, u_{n+2}, \ldots, u_6, u_4, u_2, o_{n+2}, \ldots, o_6, o_4, o_2, o_{n+2}, \ldots, o_6, o_4, o_2, t_n, t_{an}, t_n, t_{an}, d_{15}, m_8, d_1, d_{15}, m_8, d_1\}$$

Main attribute set '*A*' is processed to form encryption and decryption process data that will be used for cryptographic appliances.

3.3 Formation of Encrypted data

Main attribute set is considered as data for encryption purpose. RSA algorithm is applied on formed data to make its encrypted format [13], [14].

$$A \xrightarrow{RSA} A_E$$

To decrypt data, RSA algorithm is applied to get main attribute set [13], [14]. Main attribute set is checked to validate & authorize user.

$$A_E \xrightarrow{RSA} A$$

Communication data is delivered or retrieve using proposed encryption technique including UCTD-ABE scheme. Indirectly, encrypted data is used to identify valid user and securely transfer sensitive data.

4. Conclusion

SAP HANA's relational database management system needs to improve its cryptographic approach in data delivery and retrieval approach. Some existing attribute based approaches have played a vital role in encryption techniques. In proposed approach, attribute set elements are selected based on selection logics. These logics are based on situation, means that current time component is considered. While forming main attribute set of elements from four attribute sets, another logic is applied based on current time component. Current situation based elements selection from attribute sets enhances the cryptographic level in SAP HANA retrieval and delivery process. Using UCTD-ABE approach, security level in SAP HANA can be improved.

References

[1] Kristen, Andrea., Mack, Holger., Schroer, Tom. (2016). SAP HANA Security Whitepaper. *SAP HANA SPS11*. 1 (1) 1-15.

[2] Weide, Christian. (2014). HANA-GRC-Security. *SAP- AG*, p1-31.

[3] Hourani, Mark. (2014). Understanding SAP HANA Security Concepts and Mitigating Risks. *SAP-AG*.

[4] Rasal, Suraj, Relan, Sanya., Saxena, Karan. (2016) OTP Processing using UABE & DABE with Session Management, *International Journal of Advanced Research in Computer Science and Software Engineering*, p57-59

[5] An Oracle White Paper. (2014). Analysis of SAP HANA High Availability Capabilities. Available: http://www.oracle.com/technetwork/database/availability/sap-hana-ha-analysis-cwp-1959003.pdf. Last accessed 22nd March 2016.

[6] Intel Real-Time Business Intelligence White Paper. (2014). Security in the Cloud for SAP HANA.Available: http://www.intel.in/content/dam/www/public/us/en/documents/white-papers/cloud-security-xeon-e7-v2-sap-virtustream-paper.pdf. Last accessed 22nd March 2016.

[7] Sikka, V., Farber, F., Lehner, W., Cha, S. K., Peh, T., Bornhovd, C. (2012). Efficient transaction processing in SAP HANA database. SIGMOD Conference (p.731-733).

[8] Farber, F., Cha, S. K., Primsch, J., Bornhövd, C., Sigg, S., Lehner, W. (2011). SAP HANA Database - *Data Management for modern Business Applications*. SIGMOD Record, 40 (4) 45-51.

[9] Han, Jinguang., Susilo, Willy., Mu, Yi., Zhou, Jianying., Ho, Man., Au, Allen. (March 2015). Improving Privacy And Security *In*: Decentralized Ciphertext-Policy Attribute-Based Encryption. *IEEE Transactions on Information Forensics and Security.* 10 (3 -1) 665-678.

[10] Qian, H., Li, J., Zhang, Y. (2013). Privacy-preserving decentralized cipher text-policy attribute-based encryption with fully hidden access structure, *In*: Information and Communications Security (Lecture Notes in Computer Science), 8233. Heidelberg, Germany: Springer-Verlag, p. 363–372.

[11] Han, J., Susilo, W., Mu, Y., Yan, J. (2012). Privacy preserving decentralized key-policy attribute based encryption, *IEEE Trans. Parallel Distrib. Syst.*, 23 (11) 2162, Nov.

[12] Suraj U Rasal, Matta, Megha., Saxena, Karan. (2016). OTP system with third party trusted authority as a mediator. *International Journal of Engineering and Computer Science*. 5 (5) 16566-16568.

[13] Stallings, William. (November 16, 2005). Cryptography and Network Security: Principles and Practice. 4th ed. -: Prentice Hall. p 257-285.

[14] Zhou, X., Tang, X. (2011). Research and implementation of RSA algorithm for encryption and decryption. *In*: IEEE Strategic Technology (IFOST), 2011 6th International Forum on 2: 1118-1121.

[15] Shraddha U. Rasal, Tidke, Bharat. (March 2014). Improving Revocation Scheme to Enhance the Performance in Multi-Authority ABE. *International Journal of Computer Applications* 90 (18) 5-10.