ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

Securing Data against Storage Jamming Attack with Event Generation

G.Neelima[1] , Dr. I. Ramesh Babu[2]

Assistant Professor, Department of Computer Science & Engineering, Acharya Nagarjuna University, Andhra Pradesh, India

Professor, Department of Computer Science & Engineering, Acharya Nagarjuna University, Andhra Pradesh, India

ABSTRACT: Security is playing vital role in every organization as the changes in technology have made them dependent on information systems. The transactions of monetary values are specifically operated by banking and financial institutions of various organizations as they are prone to high risk. Online applications and authentication systems are manipulated by different attacks and intrusions by hackers. MANETs are frequently affected by different types of attacks. The most predominant one among them is Jamming Attack. In this paper we would like to focus on Storage Jamming which is being a major threat to the stored data in the databases. Initial experiments have shown that access control, encryption, auditing and virus detection do not prevent or detect this kind of jamming. Storage Jamming is the malicious modification of stored data for the purpose of degrading or disrupting real-world operations that depend on the correctness of the data. My work is to track the intruder if it attempts to read or modify the data. The mechanism that we have adopted is an improvised one with regard to efficiency and time complexity. The first step of the model is to check whether it is the intruder or the user that has tried to modify the data. If it is the intruder who tries to change the stored data in the databases, an event which we have implemented will be generated by the middleware tool.

KEYWORDS: Storage Jamming, Authentic Values

I. INTRODUCTION

Netwok security is to be considered as the first priority in the field of web applications and online transactions. Especially in every organization the security methods are highly solicited at the time of transferring the data and while storing it in the databases. Cyber-Crime is regarded as the most serious threat for financial applications and online banking applications. It is sometimes initiated by the artificial Intelligence to break all types of textual passwords. The intensity has been increased to maximum extent with the combination of different types of attacks. The wireless MANET presents a larger security problem than conventional wired and wireless networks. There are different types of attacks in MANETs which challenge their security .Some of such attacks are Guessing Attack, Dictionary Attack, Storage Jamming Attack and Denial-Of-Service attack. Jamming is a special class of DoS attacks which are initiated by malicious node after determining the frequency of communication. Jamming attacks also prevents the reception of legitimate packets which exhausts the network resources.

In particular storage jamming is a surreptitious modification of stored data, to reduce its quality. The goal of the storage jammer in general will be deteriorating the position of a competitor. These types of attacks pose a critical threat to security of Manets. The data that is stored in the databases by the authenticated user is called as authentic data or authentic values [2]. If the attacker modifies the data and stores those malicious values then they are said to bogus values.

A storage jamming attack diverges the state of the stored data from the given authentic state. The jammer modifies the authentic values with an intention that the resultant bogus values will adversely affect the victim's performance of some real world's task. The problem would be relatively high if the user continues to use the bogus data for a long time without identifying that the data has lost its authenticity. There are many possibilities open to the storage jammer. It can operate up on large databases. Some of the issues that remarkably affect the problem are the rate and extent of the malicious changes, the method adopted by the jammer, the system architecture of the target node. It is

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

very important to understand the nature of the jamming attacks in order to balance the cost of defenses against the ease of making such an attack[1].

In general, the most promising targets for storage jamming are systems with complex stored data, the authenticity of which cannot be determined by inspection. The main objective of a jammer would be reducing the quality of stored data below a certain level, without being detected. Unlike traditional method of jamming the communication systems, we assume that it is relatively better to stop the storage jamming once it is detected. The main goal of the paper is to track modifications done by the malicious node that is deployed to perform storage jamming. Whenever the jammer snoops into the network and
modifies the authentic data present in the database, with in no span of time the mechanism which we have developed will detect it. If at all detection of storage jammer is done it is easy to mitigate the jamming process.

Characteristics of Storage Jammer

In our paper we have focused on the threats to the security of database caused by the jammers. In order to detect the jammer or resist it from modifying the authentic values of database the strategies that may be adopted by a storage jammer should be characterized. This step would be useful in finding out an effective anti-jamming mechanism. The general important attributes of a storage jammer are taken into consideration [10]. They are

Sustainable Bogus Values

The unauthorized changes can be persistent or the jammer can restore the changed values after a given amount of time. A useful variation of this would be to save deleted objects or values and reintroduce them at a later time. In electronic warfare terminology this would be a form of repeat-back jamming. Interim bogus values are harder to detect but may still be read by critical applications or system programs.

Security factors

The jamming may be done by an authorized program or by an unauthorized program. If it is done by an authorized program it may be done as part of an authorized implementation, i.e the program simply writes incorrect values, or the jammer may be able to cause an unauthorized invocation of a legitimate application.

System Structure of the Target Node

The target machine may be unstructured legacy systems to modern well-structured systems. It is hard to determine the jam threat if the systems are not well structured . The modularity and encapsulation in a well-structured system isolate the effects of malicious data to a single part of the system.

The Way the Bogus Values are chosen

The jammer can adopt a number of basic algorithms for generating the data to write. The bogus values can be chosen arbitrarily, randomly, by interpolation, by replay, by permutation,etc. Arbitrary choices may be easy to detect, but can be performed by small programs that may be easier to insert into a system.

Target Authentic Data Items

The jammer can select targets randomly or through some selection criteria or by simply piggybacking on an application program. This last approach lets the application chose the target for the jammer. If the target is authentic data stored in the data bases it would be a great damage to the databases.

Class Of Target Data

The data can be application data, linkage data, metadata, or system data. A more important classification of target data is the level of abstraction. Granularity of representation has to be chosen for such type of classification. The target data

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

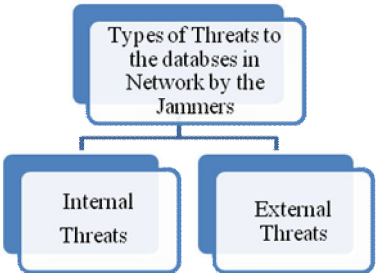

Fig 1.Types of Threats

may be the data that is stored in the relational database or could be disk blocks in the nodes of a given data structure

Rate Of Change In Target Data

If there are many updates to the data, then jamming may be easier. In such cases there will be more chances for the jammer to induce bogus values and more checks are to be done to find out the jamming.

Rate Of Jamming

The rate at which changes are made is significant. A jammer may be designed to jam as fast as possible without being detected, with the expectation that the jammer will only be triggered at a critical moment. Alternatively, the jammer may run continuously and make changes infrequently.The rate of jamming can be quantified, at a given level of abstraction, in terms of the number of data items jammed per state transition. One way to do this is view each high-level command as the input causing a state transition. Note that we include all state transitions, including those that only read data

Extent Of Jamming

A slow jammer can still do much damage by using a cumulative strategy of jamming slowly but widely, i.e. ultimately change every value stored in a database. This type of jamming is usually called barrage jamming [1]. On the other hand, there are certain set of jammers which concentrate on certain critical subsets of stored data. This kind of jamming is called spot jamming. In this paper we have worked up on spot jamming.

The basic attention is on the nature, characteristics and extent of jammer. The extent of jamming can be quantified at a given level of abstraction in terms of the number of data items jammed in a given state. In general Extent is an important issue for the storage jammer. If storage jamming is continuous, then at some point all of the data targeted by the jammer will be jammed.

We assume that at some point before the extent of jamming reaches 100% the presence of the jammer will be detected by direct inspection by the users. For this reason, we expect the jammer will stop before such a point is reached. The jammer can then wait until normal computations change the bogus values into authentic values and then start jamming again.

II. RELATED WORK

Jammer's Acquaintance with the Target Node

An enemy may hope to do more damage by having the jamming software changing its strategy. This may be a simple acquaintance with the target, such as changing the constraints that are checked while generating bogus values. It may be more complex trying to adapt to detection mechanisms that might be present. It may be necessary to prevent the jammer from reading the data or code of the detection process[3].

Types of threats

As shown in Fig 1 the threats caused by a jammer can be an internal threat or an external threat.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

Internal threat

Internal threats are likely to come from an individual who is authorized to use the authentic sensitive corporate data. This could be anyone working in the same company or a third party representative who possesses access to the corporate database.

External Threat

External threats are likely to come from the outsiders whose motive is to corrupt the data values in the database thus causing great disaster for the company. Internal Jammer has an easy means, opportunity and motive to intrude into the target node where as External Jammer will have only motive. So External Jammer may choose Spear phishing technique to easily intrude into the database.Spear phishing is an extremely affective way for hackers to get in. With this they trick an innocent employee into clicking on the malicious link, their machine can then be controlled by the outsider but with insider access[9].

In this paper we want to address the problem of modification of corporate data in the centralized databases by the jammers. Due to the vast increased storage of data in the enterprises, databases have been largely secured against intruders through network security measures such as firewalls, and network-based intrusion detection systems. While network security controls remain valuable in this regard, securing the database systems themselves, and the programs/functions and data within them, has arguably become more critical as networks are increasingly opened to wider access, in particular access from the Internet.Security breaches can harm the data of corporate network environment in a remarkable manner. It should be guaranteed that the network access is controlled through authorization, and that data is not exposed to attack when it is stored in the databases or when it is being transmitted across the network.

Ensuring Secured Connections

A middle tier can be configured that manages the connections of vast number of users. Then it is possible to filter on source, destination, and host name. We can ensure that connections come only from a physically secure terminal or from an application Web server with a known IP address. Since the intruder can use fake IP address, it is not the only factor that is to be taken into account for authentication. In the case of a sensitive database, we want to ensure that connections can be allowed from certain points in the network. For example, a company may adopt a security policy which ensures that an user John can access the payroll database, but only when he is present at work. It means that he can access the data base only being within the Intranet of the organization not even form its subnet. Virtual Private Database which plays the role of a secure application can be used to limit access to the database from particular network nodes.

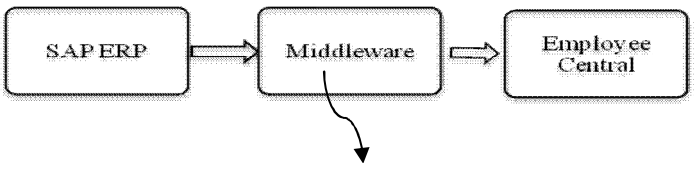

Fig 2 End Point URL in the Middleware

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

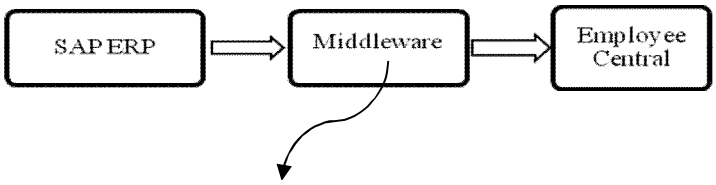

Fig 3 End Point URL in Employee Central

III. SCENARIO DESCRIPTION

In our research work we have worked up on the employee database management. For better and efficient results we have used SAP ERP software and DELL Bhoomi as middleware. ERP provides an integrated view of core business processes using databases maintained by a database management system. It uses a common database for all the applications. Dell Bhoomi is an on-demand integration tool for connecting cloud and on premises applications and data. This tool help us to transfer the data between cloud and required applications providing high level of security.

The scenario in Fig 2 and Fig 3 consists of Financial system, Employee Central and Payroll. The SAP ERP Financial system is always the master system for cost centers. Employee Central masters the assignment of an employee to a cost center. The information is passed over through employee master data replication to the Payroll/Financial system. The Payroll system is fed directly by the Financial system.

Initial Procedure to prepare the systems for Integration

Step 1: Setting up the Employee Central system
Step 2: Setting permissions for API User
Step 3: Initiating the middleware
Step 4: Deploying the integration pack

Finding the URL for communication from SAP ERP to the middleware

The integration process for cost center replication is triggered by the SAP ERP system. This means SAP ERP needs to know the endpoint URL that it is to be called in the middleware as shown in Fig …
The integration for cost center replication from SAP ERP to Employee Central triggers calls to Employee Central using the middleware. This is why it needs to know the endpoint URL that is to be called in Employee Central. The Cost center process uses the OData API.

Finding the Logon Data for communication from SAP ERP to the middleware

The integration process for cost center replication is triggered by the SAP ERP system. This means SAP ERP needs to log on to the middleware. Logon data has to be copied from the middleware system when we create an RFC connection.

Procedure for Replicating data of Cost centers from SAP ERP to Employee Central.

SAP ERP manages the database of the employees. Cost centers are generic objects in Employee Central. They are effective dated like any other master data object in Employee Central. Cost centers are used for employee assignments as well as in alternative cost distributions.
Whenever a cost center is created or modified and where it fulfills the selection criteria defined in the variant for data replication in the program, a change pointer will be written and the change pointer processing will create the IDoc and

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

send it to Employee Central. IDoc is an acronym for Intermediate Document. It is an object that carries data of a business transaction from one system to another in the form of electronic message. The purpose of it is to transfer data or information from Financial System to Employee Central. The transfer will be in the form of EDI (Electronic Data Interchange).

Process for Replicating Cost Centers

The replication of Cost Centers can be either file or message based. The file-based option is useful for a quick system setup in the beginning of the task, although it can be used to regularly update Employee Central with delta changes. This program allows downloading files directly to our front end PC as well as storing them on a server for automated distribution. To enable delta loads for both variants, file-based and message-based, change pointers are used in SAP ERP.

After setting up the Systems for integration, the endpoint URL for communication between the middleware and Employee Central is to be chosen. If needed other endpoint can also be added. To Replicate the Cost Centers first authentication is to be done.

Authentication Process

1. The ID of the Employee Central Company to which we want to transfer the data is to be taken
2. The name and password of the user who has the permission to access OData APIs is to be validated

Field Mapping in the middleware and Application Link Enabling

Table I . Informtion of IDOC

IDOC Node	IDOC Attribute	Employee Central Node	Employee Central Attribute
CostCenter Data	Remote Object ID	FO CostCenter	ExternalObjectID

To replicate the Cost Centers, the fields of Employee Central are to be mapped to the middleware.

After mapping, some configuration steps are needed to enable data distribution for cost centers using Application Link Enabling. They are

Step 1- Remote Function Call connection is to be created. It enables calling and execution of predefined functions in a remote system. It manages the communication process, parameter transfer and error handling

Step 2-Then two logical systems are defined, which represent the communication partners for the data transfer, Our SAP ERP system and the middleware system. A distribution model is to be defined, which specifies that cost center data should be transferred between these systems

Step 3-A port is to be created that uses the RFC connection that was created in the first step. The port is the channel by which the SAP ERP system can exchange data with the middleware

Step 4-A partner profile is to be created for the logical system that represents the receiver. Receiver in this context is the middleware system. In the created profile the port that was created in the first step is to be specified for the purpose of communication. The partner profile defines the parameters for the data exchange with the middleware.

IV. EVENT GENERATION BY THE MIDDLEWARE

Replication of Cost Centers is being done from SAP ERP to Employee Central so that any modification done to the ERP system will be represented in the Employee Central. This is to eliminate the ambiguity between the two

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

databases. Whenever any Cost Center is created or modified immediately it will be replicated at the Employee Central. There is no need to manually initiate the replication process. DELL Bhoomi integration tool that we are using allows us to trigger the updation or modification events. The event will be triggered with IDoc. The purpose of an IDoc is to transfer data or information from SAP to other systems and vice versa. The transfer from SAP to nonSAP system is done via Electronic Data Interchange (EDI) subsystems whereas for transfer between two SAP systems, Application Link Enabling(ALE) is used. IDoc is triggered in SAP system or in EDI subsystem.

This depends on the direction in which IDoc is sent and is called as Inbound IDoc and Outbound IDoc accordingly. In our research paper we are using outbound flow as IDoc is triggered in SAP through document message control. It is then sent to EDI subsystem. EDI converts the data from IDoc into XML or equivalent format and then sends the data to the target system through network. For the transfer of data between the source and target nodes , IDoc port is used. It contains the information about the way the data is being sent. In our research work, as we are using the port type "File", directory or file name information is maintained. IDoc structure is divided into

-Control Record
-Data Record and
-Status records

Control Record -It contains information such as IDoc number, direction, IDoc Status, Basic Type, Message Type, Partner (Sender/Receiver), date and time of creation/update, Interchange File or ISA number, etc.

Data Record - It contains the details of the IDoc segments.

Status Record - IDoc Status defines the processing status of the IDoc. IDoc statuses are used to track the IDoc and its various processing states. Status Numbers represents IDoc status. Current status of the IDoc is present in Control record

The SAP ERP system manages the database of the employees. Several research works have pointed out that the product can be plagued not only by SQL injection vulnerabilities,but also by cross site scripting vulnerabilities that allow an attacker to execute arbitrary JavaScript code. These vulnerabilities pose a serious threat to SAP customers in the form of modifications or deletions done to their existing information in the databases.

Our research paper has focused on this dimension of threat to the databases. If an intruder enters into the secure zone of the centralized system bypassing various potential authentication credentials and secured connections Event which is scheduled to be generated by the middleware is going to alarm the target node about the modifications done to the database with in no time. The target node receives the IDoc from the sender as and when the cost center is created or modified. With the Remote Function Call mechanism we can confirm the authenticity of the specific API which has created/modified the Cost Center. If it is the authenticated one who has done changes to ERP system, then the newly inserted/created values will be replicated to the Employee Central. Else if it is found that it is the intruder who has done alterations to the database, then the target node can identify all the changes done to the database by the intruder.

The detailed information regarding the changed or newly created fields can be observed and the corresponding information can be propagated to SAP ERP without updating the Employee Central with the malicious values.

V. EXPERIMENT RESULTS

The event that is generated by the web service server consists of the details regarding the node that has changed the data in the cloud database and also the fields that were changed by it. It is the responsibility of the authenticator to check whether the node is a malicious one or an authorised node.

As shown in the below figures Replication of Cost Centers from SAP ERP to EC is done using the IDoc ODTF_CCTR. Here ODTF_CCTR is an object of IDoc. The iFlow listens to incoming cost centers and whenever an IDOC is received, the processing in EC is triggered immediately. The web service server listens the IDoc cost center replication message. Mapping will be done according to customer requirement for the EC system. Mapping is needed in order to identify the fields and the customer id whose fields were modified. After that the output of the mapping will be send to EC system. Then an acknowledgement is sent from the EC system to SAP system to check whether the cost

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

center fields are replicated or not. If the modification is termed out to be a genuine process then only replication will be done.

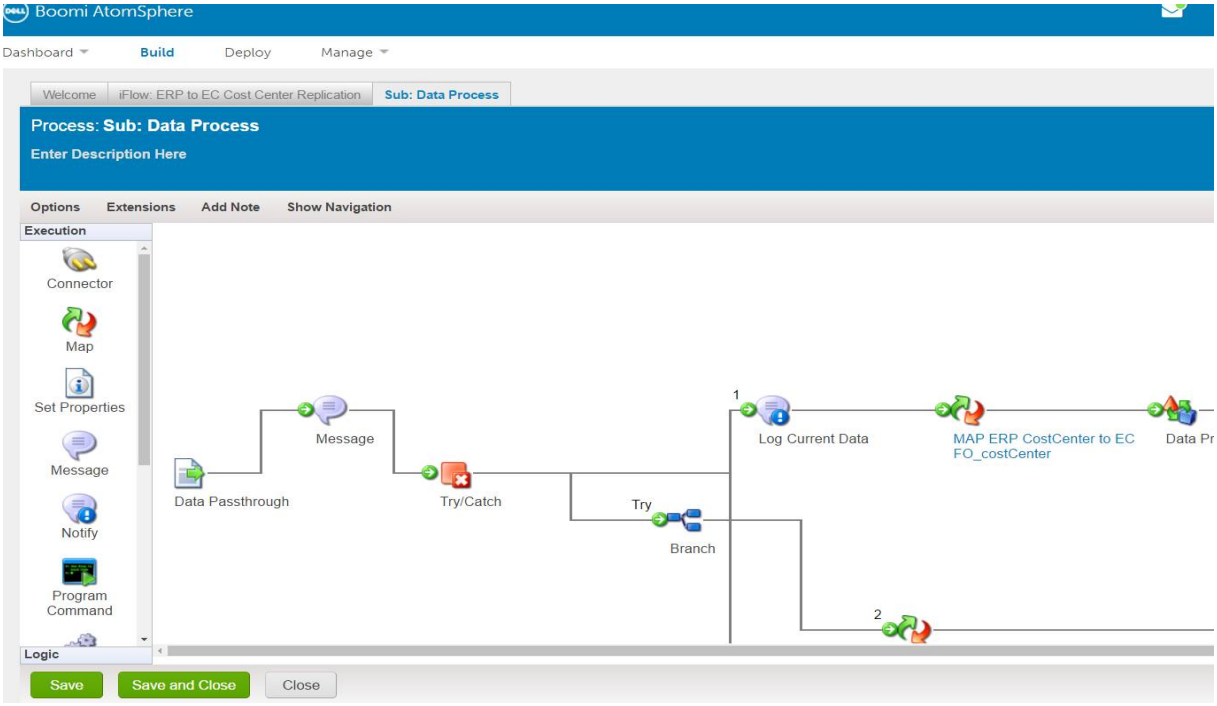

Fig 3. Replication of Cost Center from ERP to EC

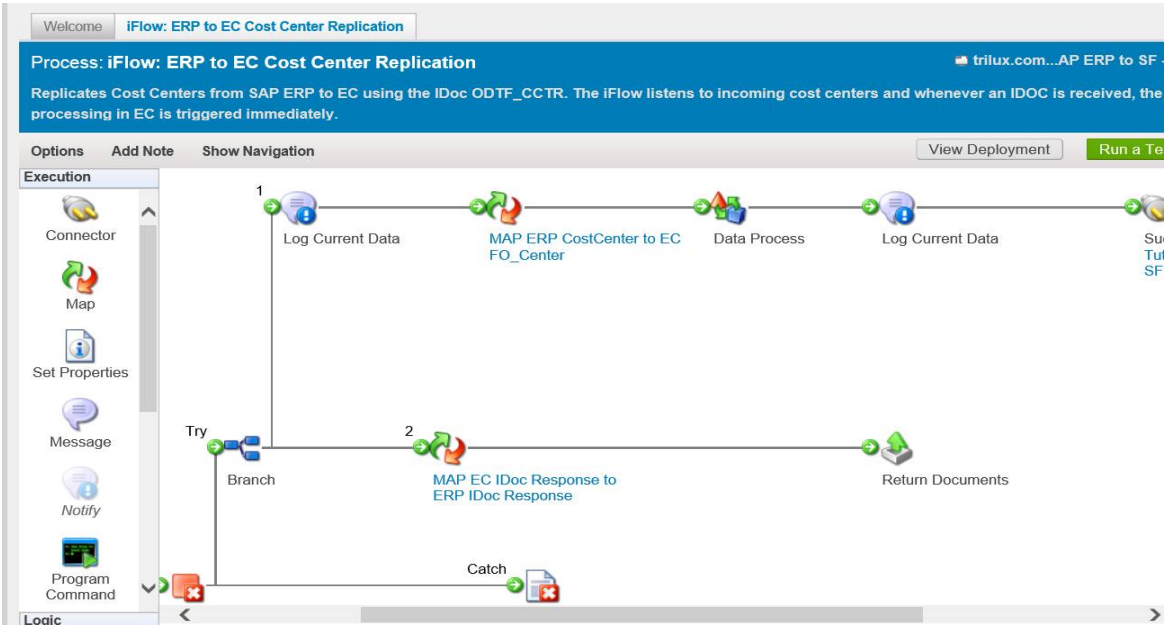

Fig 4. Processing at Employee Central

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

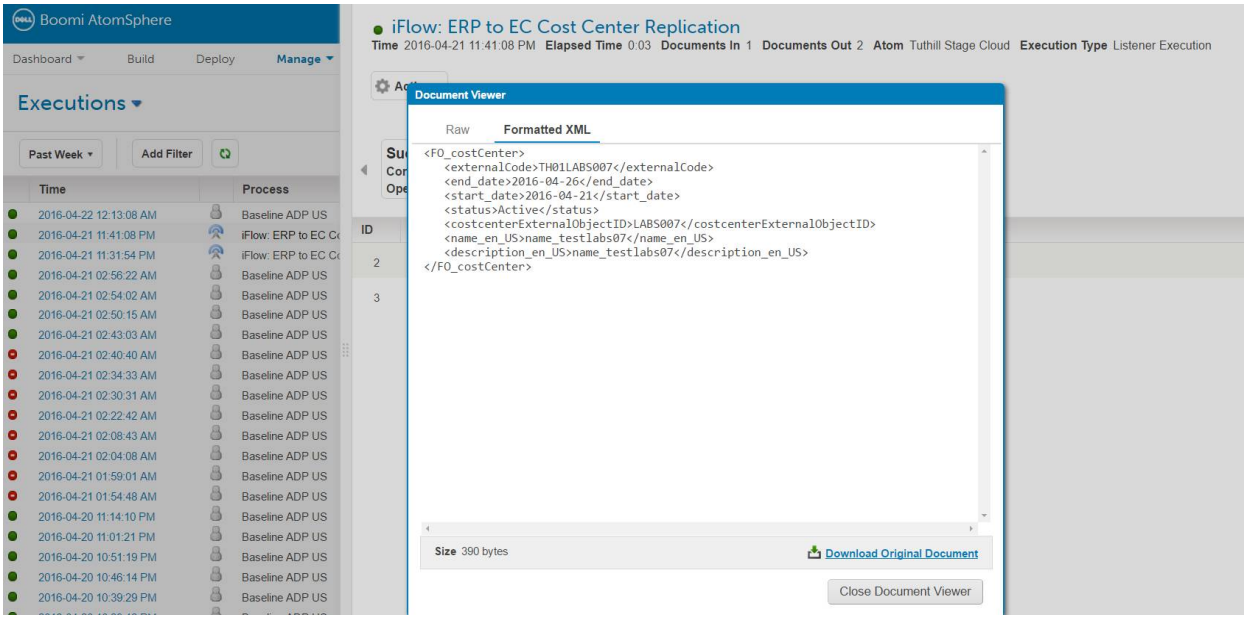

Fig 5. Object generation by Web Service Server

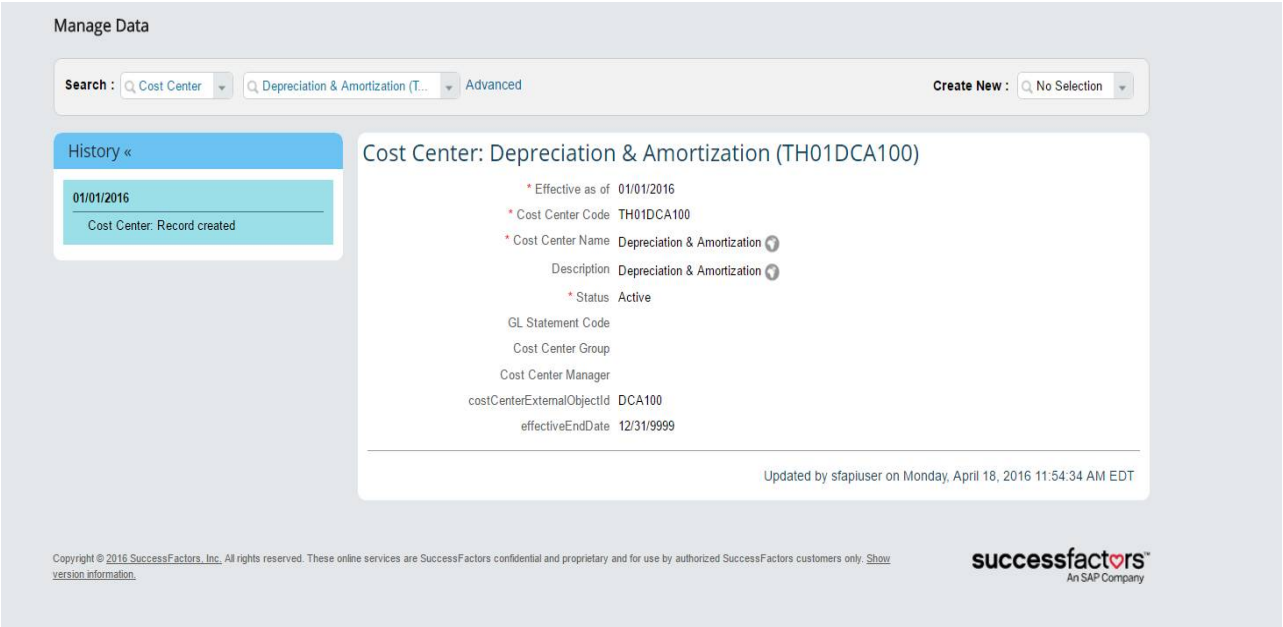

Fig 6. Acknowledgement generated by Employee Central

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

VI. CONCLUSION

In our research work we have focussed on developing a mechanism which was able to provide high level of security to the stored data in the network. In the stored databases of the network or the cloud databases if any malicious node intrudes into the network and changes the data in the system they will not be replicated in the central database of that network unless it would be identified as authorised replication. To perform that task we have created an event generation mechanism with the help of a middleware tool. An event will be generated whenever any modification or updations are done to the existing databases which is going to alert the central system regarding the corresponding changes. Then with the help of information provided by the generated event it could be checked whether the changes are done by the malicious node or not.

REFERENCES

[1]. Philippe Massonet , Anna Levin, Antonio Celesti , Massimo Villar, Security Requirements in a Federated Cloud Networking Architecture, Communications in Computer and Information Science, pp 79-88, April 2016
[2]. Luca Ferretti,Michele Colajanni,Mirco Marchetti, Supporting security and consistency for cloud database, IEEE, Feb 2014
[3]. Kanika Grover, Alvin Lim, Qing Yang. Jamming and Anti-Jamming techniques : A Survey International Journal of Adhoc and Ubiquitous computing ,pages 197-215, 2014.
[4]. Sabareesan M , Gobinathan N Network Database Security Issues and Defense International Journal of Engineering Research and Applications Vol. 3, Issue 1, pp.1748-1752, January -February 2013.
[5]. Luca Ferretti, Fabio Pierazzi, Michele Colajanni, and Mirco Marchetti, Security and Confidentiality Solutions for Public Cloud Database Services, The Seventh International Conference on Emerging Security Information, Systems and Technologies,2013
[6]. Wei She and Bhavani Thuraisingham, Security for Enterprise Resource Planning Systems, Information Systems Security, 16:152–163, 2007
[7]. H. Suo, Z. Liu, J. Wan and K. Zhou, Security and privacyin mobile cloud computing 2013,9th International Wireless Communications and Mobile Computing Conference (IWCMC), Sardinia, pp. 655-659, 2013.
[8]. T.X.Brown, J.E.James, and A.Sethi. Jamming and sensing of encrypted wireless adhoc networks. In Proceedings of Mobihoc, pages 120-130, 2006.
[9]. Kenji Hashimoto, Fumikazu Takasuka , Verification of theSecurity Against Inference Attacks on XML, Databases10th Asia-Pacific Web Conference, APWeb 2008
[10]. McDermott and J.Froscher, Practical Defenses Against Storage Jamming, DataBase Security IX, IFIP Advances in Information and Communication Technology pp 365-381