International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-9 Issue-5, January 2021

A Cloud Database based on AES 256 GCM Encryption Through Devolving Web application of Accounting Information System

Alameen Eltoum Mohamed Abdalrahman

***Abstract:** The main objective of this research is to use AES 256 GCM encryption and decryption of a web application system database called Accounting Information System (AIS) for achieving more privacy and security in a cloud environment. A cloud environment provides many services such as software, platform, and infrastructure. AIS can use the cloud to store data to achieve accounting with more performance, efficiency, convenience, and cost reduction. On the other hand, cloud environment is not secure because data is kept away from the organization. This paper focuses on how we deal with secure sensitive data such as accounting data AIS web application at web level encryption by using AES 256 GCM encryption to store data as encrypted data at cloud in a secure manner? Accounting Information System (AIS) has very sensitive data and its need to be more secure and safe specially in cloud because it's not saved at local servers but at another cloud service provider. The storage of encryption and decryption keys are stored in locations and devices different from those in which the database is stored in the cloud for ensuring more safety.*

***Keywords:** Accounting Information System (AIS), AES 256 GCM , Cloud Services, Database Cryptography*

I. INTRODUCTION

The world has changed dramatically and there has become an amazing change mainly in technology. World became a small village, Networks and Internet spread all over world with high capabilities and speeds. As a result, of expansion of Internet almost everywhere, cloud services have become available over the Internet with its various advantages and accessibility. A large number of organizations have turned to benefit from cloud services and its advantages such as cost, performance, availability and safety. AIS in an organization contains an important and big database that we suggest to be kept in the cloud environment. On the other hand, there are some challenges facing AIS database in cloud environment especially security issues related with sensitive data such as accounting which are stored in locations that are away from organizations. Security problem of AIS database in cloud can solved by encrypting database at application level to send encrypted data to cloud Best encryption method by use AES 256 GCM which it has many featured secure encryption with power of encryption and decryption. This paper focus on a cloud Database based on AES 256 GCM encryption through developing a web application of Accounting Information System. We developed a web application system using an open source with application encryption level AES 256 GCM and storing encryption DB in cloud database. Encryption and Decryption keys stored on a different server from cloud for further protection.

II. RELATED WORK

An online application store data at cloud far from organization, cloud services and AIS. There are many papers talk about encryption database, cloud services and AIS. One works describing how Cryptography DB which help with hosting databases in the cloud securely [1]. The first order-preserving scheme that achieves ideal security main technique is mutable cipher database, meaning that over time, cipher database for a small number of plaintext values change, and we prove that mutable cipher database are needed for ideal security. An encrypted MySQL database application providing ideal security, scheme achieves , high performance than encryption scheme, which is less secure than encryption scheme that computes order queries in Encrypted Data Base is presented in [2]. Cloud computing provide shared and parallel computer and storage services to be used by a multitude of clients. There is a problem of unsecure database on a cloud server, to solve this security we present an approach where agents share reserved data in a secure manner by use of authorization on shared data [3]. Data protection with privacy from threats, there are many different type of encryption models proposed, an Attribute Based Encryption (ABE) is one such interesting approach where the cipher text, the secret key and the private key of user are associated with user's attributes one example developed a system called the Cipher text-Policy Attribute Based Encryption (CPABE) for implementing using the attributes of user encrypting the document [4], [5], [6]. Most of related work focus encryption by different ways but we proposed AES256 GCM because it has many feature that are more secure in our view related of encryption and key encryption key.

III. METHODOLOGY

Methodology at paper take two sides descriptive and Experimental approach, Descriptive approach referred to some papers & references through literature on AIS, database , Encryption and cloud services. Experimental approach through AIS web application through open source and applied AES256 DCM Encryption of Database that are stored on Cloud and generated encrypt & decrypt keys which stored at different server of cloud.

Manuscript received on January 18, 2021.
Revised Manuscript received on January 22, 2021.
Manuscript published on January 30, 2021.

Alameen Abdalrahman, Assitant Professor Jouf University (Saudia arabia)& Neelain University (Sudan)

IV. ACCOUNTING INFORMATION SYSTEM

Accounting Information system (AIS) have many definition most definition AIS is a collection of resources, such as people and equipment, that are designed to transform financial and other data into information [7] [8] [9].

The objectives of AIS are to collect, process and produce any information that is relating on financial aspects of business activities [10]. Information system can also be defined as an effective and improved way to control the users efficiently [11]. Nowadays, AIS can be defined as simply AIS is a collection of Items which work together to achieve goal of accounting this items contain hardware, Software, procedures, users and data. It can be concluded that AIS is a group of some elements that manage the recording into the accounting information useful for the users of Information. AIS on the basis of above opinion is a collection of integrated system that manages financial transaction data into the financial statements using modern technology.

V. CLOUD SERVICES

Cloud services is a new technology that provide many services such as application, platform, and infrastructure. Cloud technology depend on network model mainly the Internet, which is working in collaboration of Parallel and Distributed Computing. Cloud services can take on demand anywhere and any time. Through internet, cloud can provide service to tens of millions of clients and retrieve information in a few seconds, therefore receive services as strong as super computer[12]. Cloud based on the location can be divided into Public, Private, Hybrid, and Community. While Cloud services based on services divides it into three main or major categories described below:

A. Software as a service mode (SaaS)

Cloud service provider provide software as a service in which cloud can provide different type of software from big to small software. Some of Saas example like Email, CRM, ERP, communications and games.SAAS can purchased from cloud provider we are found many solutions in different area, AIS and financial Systems is an example of SAAS service which can offer from cloud provider to client as paid service with all working related to accounting and financial with fees depend on software service types, quantity, quality, features, duration and other elements while clients obtain their needed AIS software services [13]. Although there are many features of SAAS product we didn't depend on it for many reasons, one of the reason SAAS solution can't allow to add many features such as adding encryption method to product without compatibility and licenses with product or not and with all company and organization freedom to select and to secure encryption method. So we didn't use Software cloud service because already developed our AIS web application and easy to add our encryption AES256GCM Through system developed by an open source PHP and MySQL so no need for software service from cloud service provider. .

B. PLATFORM AS A SERVICE (PAAS)

Platform as a Service (PaaS) provides a platform as a service, include Cloud Computing development and operating which is already or product of SAAS. PAAS have different plat form such as web server, database, execution time and financial system development. Platform resources support development language and tool, to develop software and program such as financial application and release it to cloud infrastructure, and then transmit it directly from servers platform to clients through the network of the supplier server [14]. Our web application depends on Platform service because we store database at cloud database, while AIS web was prepared encryption data and migration data to cloud database. Application was developed with an open Source manually programmed and Database cloud service must provide by PAAS provider.

C. INFRASTRUCTURE AS A SERVICE (IAAS)

IaaS (Infrastructure as a Service) firstly let us know what the mean of infrastructure, it means virtual machine, network, storage, server, data center and rest of computational resources. Infrastructure is a paid service to clients. Clients can run its own AIS applications in the cloud infrastructure [15]. Cloud service provide an Infrastructure as a service (IaaS) to store our Database. Storage of cloud with different advantage of cloud by availability, capacity and on demand service. AIS web application Encrypted data migrated to cloud service provider which hosts AIS Database but encryption and decryption key must be at another server.

VI. CRYPTOGRAPHY DATABASES

Cryptography databases Usually Used to secure data base for protection main properties of database such as Confidentiality, integrity and availability. In cloud environment Such as database on PaaS which is not assured in the outsourced data centers, where the platform as a service (PaaS) provider is external to data owner of database. A good method to solution this problem is t encrypted database that only treated by DBMS. There are three main categories of database encryption [16].

A. Storage level encryption

Storage level encryption (SLC) encrypted data when data store at storage devices. It prevents theft of storage but it is preventing unauthorized access, On the other side, it is entirely transparent to the system, so it needs no database modification [18]. Our proposed database didn't depend on this type of encryption level because already storage at cloud storage which responsible for Cloud service provider.

B. Database-level encryption (DLE)

Database level encryption (DLE) is used to secure data in database when read and write of a database. The encryption is applied to the DB at all level of DB such as database, tables, columns and rows we mentioned that the most frequently is columns. It can be related with some logical conditions for selecting affected data .[18] Our paper focus on Database level Encryption that are created at web application system to store encrypted database in cloud. Although this type of encryption is secure but it effects on performance such as slowed down as a result of overhead.

C. Application-level encryption (ALE)

In this case, data is encrypted/decrypted by the application, and the data sent to database is encrypted while over the network.

In cloud environment this scheme is acceptable regard that data stored at remote site at cloud so we ensure encrypted data from application and sent encrypted data over network the manager ,owner and system developer can selected which encryption type suitable for the system and they can control encryption [18].

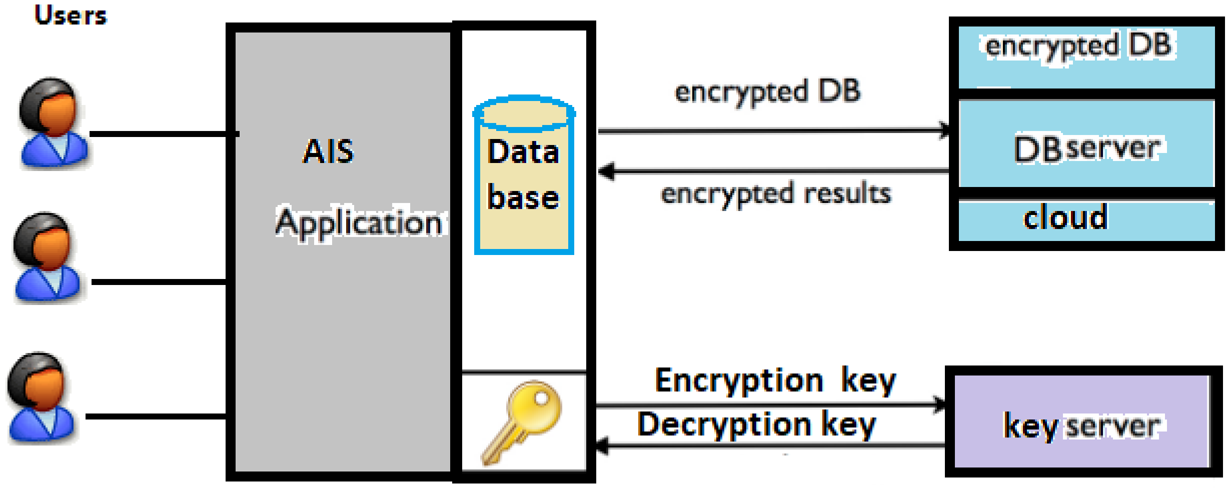

Fig. 1: System Architecture

VII. PROPOSED SYSTEM ARCHITECTURE

AIS authenticated user before login to system, user can insert plain text to system As shown in Figure 1 [19].
AIS Data base contain many tables, one of most important table of DB is Journal Entry as shown in table I) simply is calculated of the credits and debits of DB transaction. Journal entry very important cause it allows organizing transactions with manageable data. Other tables in AIS DB are depended on journal entry so it post data to general ledger tables and other tables. In this part We take journal entry table as Example to encrypt & decrypt database. We take journal entry as the main table in systems which all other tables are generated data from Journal Entry. Regarding that data stored at remote site at cloud, so we ensure encrypted data from application and sent encrypted data over network the manager, owner and system developer can selected which encryption type suitable for the system, and they can control encryption [18]. The database encryption are divided into two main category Symmetric and Asymmetric below more detail about them[21][22][23][24]:

Table- I: Journal Entry table –main table in DB

JNO	Jacc	Date	Account	Debit	Credit	Explanation
1	234	03-03-202	Prepaid rent	**36,000**		Value : $36 thousand paid advance rent.
2	345	03-03-202	cash		**36,000**	Value : $36 thousand paid rent
3	654	04-09-202	Office Supplies	**17,600**		Purchased office costing $17600
4	345	04-09-202	Accounts Payable		**17,600**	Purchased office costing $17600

A. *The Symmetric database encryption*

Symmetric encryption depends on one key called a private key, It being applied to data that is stored in database and called when decryption from a database. The data altered by private key which mean data converted to Incomprehensible and encrypted [20]. Data migrated and saved to cloud is encrypted data, the user restore data by using private key, Secret key used by the sender and receiver to decrypt and view the data [21]. Symmetric encryption an advantage has that only one key in the encryption process so it speeds and less storage cost of symmetric encryption.[22]. In another hand disadvantage Sensitive data may be stolen or exposed if the private key is released to people who do not have access to the data [20].

B. *Asymmetric database encryption*

Asymmetric encryption consists of two different types of keys, private and public keys [23]. Anyone can access the unique key, which is the public key, and it is for one user, while the private key is a secret and unique key and only for one user [24]. The public key is the encryption key while the private key is the decryption key, Asymmetric encryption is often described as more secure for symmetric database encryption because the interaction is with two separate keys with the encryption and decryption operations, for performance reasons, asymmetric encryption is used in key management. Instead of encrypting the data, it is usually performed using symmetric encryption [26] [25]. We depend on AES 256 GCM encrypt & decrypt database One of the main reasons is the encryption system. I created the current version years ago. At that point, using mcrypt was recommended on the internet application. However, since then mcrypt has become deprecated and has been removed in some versions. Because the encryption is essential to the system and very hard to change after the fact, I spend a few hours reading up on the current best practices for symmetric encryption in and ended up with
AES 256 GCM.

Encryption and Decryption technique using PHP.
Encryption with base64_decode key as shown in table II for of Journal Entry table Suppose that column Debit of Journal Entry Table as shown as Figure 2 by following steps:
1. User Login Authentication.
2. encryption decryption (AES 256 GCM) method.
3. Key encryption and decryption base64_decode
4. Function we use for encryption openssl_random_pseudo_bytes()
5. Insert key by MySQL code to key server
6. Insert encrypted data base to cloud database SERVER.

In the other hand decryption, we use following steps:
1- Login Authentication.
2- Retrieve decryption key from Server Key.
3- Retrieve Encryption database from cloud database.
4- Decryption (AES 256 GCM) method for Encryption database using Decryption key.
5- Function used for decryption with decryption keyopenssl_random_pseudo_bytes(openssl_cipher_iv_length()
6- Result of process is plain text of Database.

C. *AES*

Advanced Encryption Standard (AES), AES is standard encryption method for many organizations. In the old mcrypt based version, there is Rijndael 128 CBC. AES is a subset of Rijndael and sometimes the names are used interchangeably. AES always has 128 block size, 192, and 256-bit keys, while Rijndael is defined for all block sizes and keys from 128 to 256 in 32-bit increments. AES 192 and 256 are also used for documents with the highest security clearance in the US. There are a few theoretical attacks to AES, but none of them is practical with current hardware. Because of its high security and wide support, AES is the logical choice for an encryption algorithm [20][21][22][23[24].

D. *GCM vs CBC*

There are many differences between CBC and GCM which are different forms of AES algorithm. CBC several attacks have been discovered on it, but it is still safe enough in most of the solutions, but I advise using GCM for a number of reasons, the most important of which are[20][21][23][25][26]:
1- GCM is considered safer.
2- GCM has a built-in authentication check, which means it can confirm the integrity of the message.
3- GCM the encoding and decoding can be parallel, whereas in CBC only decoding can be parallel.
4- GCM Encrypting large files can be much faster on multi-core CPUs.
5- GCM can Run many programming language such as PHP and can be done using OpenSSL so It can run GCM, and I don't need it for the small message.
6- GCM has great security than CBC.

The biggest difference between CBC, GCM is the requirements of (IV), where CBC requires a strong IV randomization, but in the case of using a sub-random algorithm it may become weak and it is noticed that GCM has great security and it is possible to use a graded IV counter to use the coding system for websites, web and applications The built-in counter is difficult to track for all sites, however the length IV of AES 256 GCM is 96 bits to be safe, there is very little chance that the same random IV will be chosen [20] [21] [23] [25] [26].

E. *Key Length*

A higher key length of 256 bits in the new OpenSSL encryption compared to 128 bits in the mcrypt version. 128-bit keys are still secure enough, especially when used with the added security of GCM. Many companies use AES 128 GCM because of its higher speed compared to AES 256 GCM [21][22][24][26][27]. AIS system which I developed depends on 256 bits by AES 256 GCM To allow users provide more secure version from server performance and secure.

F. *Algorithm AES256GCM Encryption Database depend on Unique Master Key .*

Algorithm AES256GCM based on unique and changeable Master Key (Mki) with more secure key by change the encryption key continuously. Lifetime (LT) end for Mki to be that new key should be created .

Scenario start with the master key the create an number called Finite Number (FN i) for encryption this number is unique number .

An Initialization Vector (IV_i) it's the same of Finite Number(FN i) and already used one time to ensure not duplicate encryption key .

Firewall (Fwi) use AES256GCM With IVi and create encryption data which encrypted with unique key.

The system need to change master key continuously to ensure IVi change which is used at encryption with AES256GCM.

The firewall should ensure non-duplication by ensuring that validated cipher with the same IVi and the same key can be generated on more distinct sets of input data of no more than 4.2949673×10^9.

The ideal to change Master key is to set timer or suggested time called Suggested time (ST) and reminder the master key with ST to be changed .

Below I represent the algorithm AES256GCM Encryption depend on Unique Master Key as follow :

```
{
Mki={ Mk1, Mk2, Mk3, Mk4,…………., Mkn}
FN i={ FN 1, FN 2, FN 3, Mk4,…………………., FN n}
IV i={ IV 1, IV 2, IV 3, IV4,…………………., IV n}
Mki create unique (FN i)
IVi =unique (FN i)
Fwi =  Enci(AES-256-GCM,unique(IVi))
Fw =  Enc1(AES-256-GCM,unique(IV1))
Loop encrypted data with IV1  for values.
If (LT(Mk1)=0) then  {   //   reminder life time
        // when applicable master key change master key
New Mk2 created
New (Mk2)= new create unique (FN 2)
IV2 =unique (FN 2)
Fw =  Enc2(AES-256-GCM,unique(IV2)) }
….
}
store data encrypted to a cloud database
Store key IVi   at server.
}
```

VIII. SYSTEM IMPLEMENTATION

AIS Application developed in PHP and Mysql as an open-source web application developed to encrypt Database before delivery to the cloud .

To develop web Application depend an open-source PHP and Mysql which provide web development support. Dreamweaver tool management system its open-source, free and quick assisted tool to design application . PHP is used in querying and manipulating the Database MySQL. To encrypt the data and AIS tables, an open-source library called openssl_random_pseudo_bytes is used which encrypt sensitive data for key we used base64_decode ( ) like journal entry data in my php powered website before entering into the Cloud database.
The Encryption library is used for carrying out the encryption which already added to PHP and Mysql .
AIS application Begin with authenticate and authorize the user. If the user allow permission, user insert data to form before database the application automatically converts user data to encrypted data by generated key for encryption and decryption after that user submitted data to store data. The data of database migrate from user application to cloud database and encryption key save at another server which is concern with store keys.
If an attack is made on the database, it is not useful because already data is encrypted so need again to attack both key serve and cloud server to take the original database.
A scenario AIS system collect Accounting Data and encrypt data to store them in a cloud database hosted on a server different than the web server. The encryption keys should be stored at least on the web server, never on the cloud database. The web server should be running a decent Web Application Firewall to keep it as safe as possible.
There isn't anything special about the implementation. Unlike GCM creates an authorization tag on encryption that needs to be provided to the decryption function, but like the IV it doesn't need to be secret so it is appended to the result. A change from the mcrypt version is the use of base64 encoding by stored the binary in DB , but whenever I had to look at the database the formatting was completely messed up. Base64 encoded text, on the other hand, is human readable and makes the database prettier to use a bit more storage space.

A. Proof of Concept

A PHP Code used to convert data from formal database to encrypted database we depend on many built in function that already with library at PHP example openssl_random_pseudo_bytes(.) it's used for encryption and base64_decode ( ) to generate keys code use MySQL command to insert and retrieve data to cloud servers and key server . As example Journal Entry table which main table in DB shown at table (1) after added AES 256 GCM encrypted In column Debit of Journal Entry table and shown at figure (2).

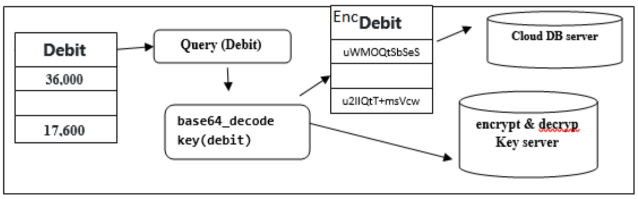

Figure2: Encryption column Debit of Journal Entry table and key encryption

B. *Sample of Code PHP codes with AES 256 GCM :*

```
function Encryptinon ( Debit , key )
{method = 'aes-256-gcm';
   key = base64_decode ( key );
   iv = openssl_random_pseudo_bytes(
openssl_cipher_iv_length( method ) );
   tag = ""; // openssl_encrypt will fill this
   res = openssl_encrypt( account , method , key ,
OPENSSL_RAW_DATA , iv , tag , "" , 16 );
   return key( iv. tag. result );
Mysql="insert into key @key server key values ( );"
Mysql="insert into journalentry @cloud database encdebit
values ( );" }
function Decryption(endebit , key )
endebit="Select debit from journalentry @cloud database "
;
{ method = 'aes-256-gcm';
   encdebit= base64_decode( encdedit );
   key = base64_decode( key );
   ivLength = openssl_cipher_iv_length( method );
   iv = substr(encdebit , 0 , $ivLength );
   tag = substr(encdebit, $ivLength , 16 );
   Debit = substr(encdebit, $ivLength+16 );
   return openssl_decrypt(debit , method , key ,
OPENSSL_RAW_DATA , iv , tag );}?>
```

IX. RESULT AND DISCUSSION

The use of IT in the world is substantial but improvement in accounting skills and technology is essential. Infrastructure of IT specially cloud services exactly at areas that are still in an infancy stage. So, the improvement of the cloud infrastructure is essential to make its use more substantial and improve in the cost, availability accountability, and support in the achievement of goal and service quality. The results of AIS cloud Based substantially helps in the achievement of target and improve in service quality but there are some Issues of security because data are store far from organization . Regarding this data are untrusted so we need to encrypt data to save it before inserting to cloud improves AIS based cloud with encryption guarantee to safety data and make use of cloud services more effectively. Thus, this study confirms to the theory of decision making. The research focused specifically on the Encryption Database for Cloud Based form Accounting Information System, and it is of immense importance to utilize it.
We focused on the following points:

1) AIS contain sensitive data so we need more secure mechanism to protect data specially when we use cloud environment.
2) Cloud provide many services such as software, platform and Infrastructure.

3) Cloud environment take the advantages like cost , performance, availability but safety of data on the cloud is very important.
4) AES 256 GCM is the best choice for the encryption & decryption of a database in a cloud environment.

X. CONCLUSION

In this paper, an AIS web application was developed in which Database is cloud-based and encrypted using AES 256 GCM for managing, access and control data security at cloud environment . AES 256 GCM encryption is used by an open-source PHP code to convert database data at application level before deliver database to cloud for guarantying more secure and easy to use user interface system.

FUTURE WORK

In future, we plan to create a new encryption algorithm for are more complex encryption and decryption database. We can measure amount of encrypted data with the plain database and the effect that with performance and cloud storage cost. Another issue we plan to work in the future is an approach of storing data at a key encryption server and at the cloud servers there is a synchronization mechanism using a form of group encryption. We are going to compare the complexity of the solution with the group encryption effort to evaluate which are the parameters that affect the performance of the two alternatives.

ACKNOWLEDGMENT

This research was supported by Jouf University, Ministry of Higher education & Scientific Research of Saudi Arabia. We grateful our colleagues who helped me and provided their opinion that greatly help me to achieve my research.

REFERENCES

1. Carlo Curino , Evan P. C. Jones, Raluca Ada Popa, Nirmesh Malviya, Eugene Wu, Sam Madden, Hari Balakrishnan, and Nickolai Zeldovich. Relational Cloud: A Database-as-a-Service for the Cloud. In Proceedings of the 5th Biennial Conference on Innovative Data SystemsResearch (CIDR 2011), Pacific Grove, CA, January 2011.
2. Raluca Ada Popa, Frank H. Li, and Nickolai Zeldovich. An Ideal-Security Protocol for Order-Preserving Encoding. In Proceedings of the 34th IEEE Symposium on Security and Privacy (IEEE S&P/Oakland), San Francisco, CA, May 2013.
3. Ernesto Damiani, Francesco Pagano Handling Confidential Data on the Untrusted Cloud: An Agent-based Approach CLOUD COMPUTING 2010 : The First International Conference on Cloud Computing, GRIDs, and Virtualization - ISBN: 978-1-61208-001-7.
4. V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,”.
5. J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attributebased encryption,”.
6. B. Waters, “Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization,” in International Workshop onPublic Key Cryptography.
7. O’Brien, J.A., Marakas, G.M., Management Information System. 10th edition McGraw Hill/Irwin, New York, 2011
8. Romney, B.M. & Steinbart, J.P. Accounting Information System. 12th edition. Pearson Education Limited, 2012
9. Stair, R.M. & Reynold, G. W., Fundamental of Information System, 6th edition Boston, Cangage Learning, 2012
10. Gelinas, Ulric J. & Richard B. Dull. Accounting Information System. 7th edition. Thompson. South-Western, 2008
11. Azhar Susanto. Sistem Informasi Akuntansi: Struktur Pengendalian Resiko Pengembangan. Lingga Jaya, Bandung, 2013 .
12. H. Gao, T. Chen, J. Lam. A new delay system approach to network based control. Automatica. 2008, 44: 39-52.
13. F. Liu, H. Gao, J. Qiu, S. Yin, T. Chai, J. Fan, Networked MultiMate output feedback control for set points compensation and its application to rougher flotation process, IEEE Transactions on Industrial Electronics,61(1):460-468, 2013.
14. S. Ding, P. Zhang, S. Yin, E. Ding , An integrated design framework of fault-tolerant wireless networked control systems for industrial automatic control applications, IEEE Transactions on Industrial Informatics, 9(1): 462-471, 2013.
15. Yanchang Kuang, “Study on the Counterplan of the Application and Development of XBRL in Our Country at Present,” Value Engineering, vol. 5, pp. 103–105, 2011.
16. L. Bouganim and Y. Guo, “Database encryption,” in Encyclopedia of Cryptography and Security, Springer, 2010, 2nd Edition
17. E. Damiani, S. De Capitani Vimercati, S. Jajodia, S. Paraboschi, and P. Samarati, “Balancing confidentiality and efficiency in untrusted relational dbms,” Proceedings of the 10th ACM conference on Computer and communications security, ACM, 2003, pp. 93-102
18. Francesco Pagano, Davide Pagano October 2011 Conference: Securing Services on the Cloud (IWSSC 2011 1st International Workshop on Securing Services on the Cloud (IWSSC), A Distributed Approach to Privacy on the Cloud “Using in-memory encrypted databases on the cloud” .
19. M. Joshi, S. Mittal, K. P. Joshi, and T. Finin, “Semantically rich,oblivious access control using ABAC for secure cloud storage”.
20. "Description of Symmetric and Asymmetric Encryption". *support.microsoft.com*. Retrieved October 25, 2015.
21. "How Encryption Works". *HowStuffWorks. April 6, 2001*. Retrieved October 25, 2015.
22. "Asymmetric vs. Symmetric – Hacking with PHP - Practical PHP". *www.hackingwithphp.com*. Retrieved November 3, 2015.
23. "How Encryption Works". *HowStuffWorks. April 6, 2001*. Retrieved November 1, 2015.
24. *Young, Dr. Bill.* "Foundations of Computer Security Lecture 44: Symmetric vs. Asymmetric Encryption" (PDF). *University of Texas at Austin. Archived from* the original (PDF) *on March 5, 2016*. Retrieved November 1, 2015.
25. "What is asymmetric cryptography and how do I use it?". *Two Factor Authenticity*. Retrieved November 1, 2015.
26. "Advantages and Disadvantages of Asymmetric and Symmetric Cryptosystems" (PDF). *University of Babylon*. Retrieved November 3, 2015.
27. J. Beth encourt, A. Sahai, and B. Waters, “Cipher text-policy attribute-based encryption,” in 2007 IEEE Symposium on Securityand Privacy (S&P 2007), 20-23 May 2007, Oakland, California, USA.IEEE Computer Society, 2007, pp. 321–334.

AUTHORS PROFILE

Dr.. Al alameen Mohamed Abdalrahman, Assistant Professor of Computer Information Systems, recently worked at Jouf University (Saudi Arabia) Faculty of Science and Arts Tabarjal ,Department of Computer Science and Neelain University (Sudan), College of Computer Science and Information Technology, Department of Information Systems. His areas of research include: Information systems, cloud computing, , systems development, Encryption and database.