A Secure Crypto-Based Data Outsourcing Model For Monitoring The Smart Environment In Cloud

A.S. Kalyana kumar, DR. T .Abdul razak

Abstract: With the massive growth in cloud computing, the data owners are interested in outsourcing their databases to the cloud. But the owners and the service providers have some hesitations to trust this domain. Thus it is mandatory to provide data privacy for sensitive data.However, encrypting these private data before outsourcing makes data utilization a difficult task. Several encryption based algorithms were developed by researchers to transfer the data securely from end to end. But existing works focused mainly on single dimensional query or undergo insufficient security guarantee, etc. Thus to overcome above challenges and to monitor the data transmissions in smart environment, a Secured Crypto based Data Outsourcing Model (SCDOM) is proposed. This paper utilizes privacy preservation scheme for detecting anomalies, an enhanced Blowfish technique for implementing encryption and decryption. Here, while receiving user encrypted data, MAC- Message Authentication Code is generated and then transmitted to Third Party Auditor(TPA) for verification. Once keys are verified, the private details are transmitted. From the experimentation results, it is observed that proposed SCDOM provides enhanced results than the conventional methods.

Index Terms: Blowfish Encryption, Cloud, MAC, Privacy Preservation, Smart Environment, Security, TPA, and k-anonymity

1. INTRODUCTION

Cloud computing [1]has an established remarkable attention in academics as well as in industry. It is more like a shared computation model above a distributed pool of virtual computing resources. These resources are processing power, storage, services and applications. It contains number of advantages for cloud users such as reduction in expenses on software, hardware and other paid services, easy accessible of wide range of applications with low management overheads, etc. But a recent survey represented that 87% of cloud users concerned about the security issues like integration in outsourcing the files, etc. However, the cloud server should not be fully trusted, as it is not necessary for the server to report incidents like loss of data. As the size of the data in cloud is high, checking the integrity leads to high bandwidth cost. Also, conventional cryptographic techniques like hash functions couldn't applied directly for verification. Thus the secured cloud storage is a muchneeded as well as a challenging topic. The smart city environment[2] is an upcoming prototype that influences several promising techniques like CPSs (Cyber Physical Systems), IoT, big data, etc. which supports intelligent services and promote a very comfortable life for residential people. It combines potential computing systems for sensing the physical changes from cities and provides feedback to world. However, people may suffer from privacy and security related threats because of the vulnerabilities caused by malicious attackers. These attackers might create false data by manipulating the sensors, launches DoS attacks, etc.[3]explained about privacy preservation and respective techniques. As the protection of private data is existed everywhere, the normal sensitive data is treated as a confidential one. This can be attained by using various encryption techniques. These techniques focus mainly on protection towards queries, access pattern, and user identification. In data security, encryption and decryption plays an important role. Encrypting the data starts with transfer of 64 bits plain text into 64-bit cipher text. These 64-bits are split into similar sized members. These 32-bit members form the base of Blowfish algorithm[4]. Some of the benefits of using Blowfish algorithm such as encryption done at a rate of 18 clock cycles faster than IDEA, DES, etc, algorithm is royalty free and unpatented, simple architecture and easy application. Once the encrypted message is received, MAC should get generated. The process of MAC is explained as follows[5]. Using MAC algorithm, a MAC value is generated and the sender transfer the message along with that value. On receiving the message, the receiver uses the input and the share key into MAC algorithm and reevaluate the MAC value.If both the MAC values aresame, then it will be authenticated. The responsibilities like checkingthe integrity of the data and saving the computational resources are done by Third-Party Auditor (TPA) [6]. This expert is differed from other ordinary users who generally verifies the data integrity in the cloud from time to time. This approach offered the file owners to be certain that data integrity is not compromised.

While securing the data, some of the problems were identified in existing methodologies as below,

- ➢ It is very difficult to detect the anomalies while transmitting the data. It is hard to achieve data anonymity and unlinkability between the files.
- ➢ Complexity in encrypting and decrypting the data.
- ➢ Data integrity must be checked.
- ➢ Some of the approaches lead to increased computational complexity and higher execution time.

In this proposed scheme, privacy preservation method is utilized for detecting anomalies. For encryption and decryption, Blowfish technique is implemented. Here, while receiving user encrypted data, MAC - Message Authentication Code is generated and then transmitted to Third Party Auditor (TPA) for verification. Once keys are verified, the private details are transmitted.

- *A.S. Kalyana kumar is currently pursuing Research Scholar, Department of computer science and engineering, BHARATHIYAR University, Coimbatore, India.*
- *DR. K .Abdul razak is currently pursuing Professor, Department of computer science and engineering,Jamal Mohamed College, Tiruchirapalli, Tamil Nadu, India.*

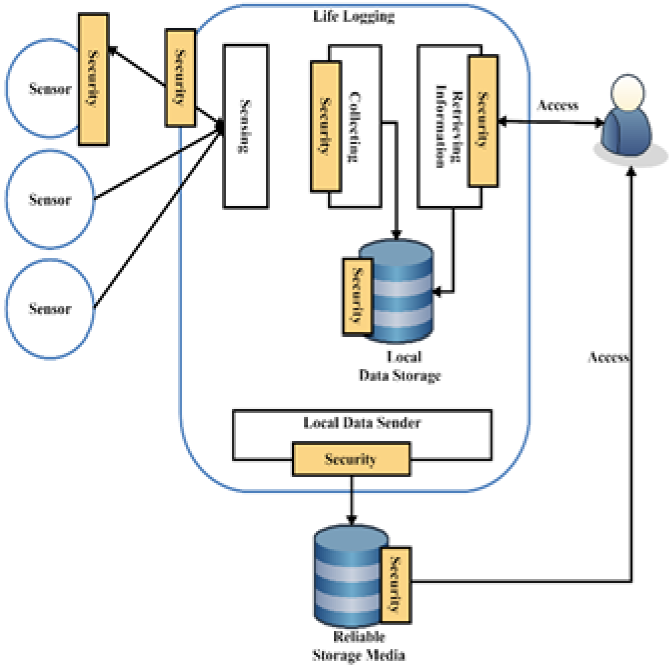

Fig 1. *Life logging*

The objectives of proposed system are summarized below,

➢ To detecting the existence of anomalies using Privacy Preservation method and to obtain privacy and security by utilizing k-anonymity.

➢ To encrypt and decrypt the messages, an enhanced blowfish algorithm is used.

➢ To maintain data integrity, MAC values are generated and will send across TPA.

➢ To reduce the computation complexity, time, and cost, this light weight model is utilized.

The rest of sections present in the paper are structured as follows: the existing architectures, and methods related to secure data outsourcing in cloud are surveyed in Section II. The clear description about the proposed methodology with its flowis presented in Section III. The results of existing and proposed techniques are evaluated and compared by using various performance measures in Section IV. Finally, the paper is concluded and the enhancement that will be implemented in the future are stated in Section V.

2 RELATED WORKS

Jacobsson, et al [7] analyzed the security and privacy risks related to the software components in the Smart Home Automation System (SHAS). In this system, the connected devices were distributed across multiple hardware solutions. Here, the risk was classified into low, medium, and high based on the mean probability and consequence values of the risk. The components that involved in the suggested architecture were, in-house gateway, connected sensors, cloud servers, mobile devices app, and mobile device. The drawback that behind this paper was, it required to utilize an automated and integrated risk analysis tools for general observation. Kumar, et al [8] designed an Anonymous Secure Framework (ASF) for providing an efficient key agreement and authentication. Here, the anonymity and unlinkability of the devices were analyzed by using a compromised session key. The major contributions were reduction in computational cost and analyzing the security strength by using AVISPA. Moreover, three different entities werecomprised in the Home Area Network (HAN) i.e. smart appliance or object, Home Gateway (HG), and security Service Provider (SP).However, this paper failed to prove the effectiveness of the suggested system. Wang, et al [9]recommended an Identity Based Data Outsourcing (IBDO) scheme to identity data outsourcing in cloud. The major contributions of this paper were to securely outsource the file to a remote cloud server based on the authorized proxies, and to efficiently verify the auditor by implementing a strong auditing mechanism. Also, the authors of this paper examined the proof of storage in cloud based on the multi-user setting. Moreover, the file owners were allowed to delegate their out-sourcing capabilities to proxies. Then, the public auditor verified both the file origin and integrity of the public auditor. However, this paper failed to reduce the computation complexity of the system. Alabdulatif, et al [10] recommended a lightweight homomorphic encryption to detect the anomalies in cloud with the use of privacy preservation mechanism. Here, both the data security and privacy were ensured by using the suggested encryption mechanism. Also, the tradeoff between the performance efficiency and computational capability was analyzed by using the Domingo Ferrer's scheme. The Fuzzy C-Means (FCM) clustering technique was employed to identify and to detect the anomalies in a distributed manner. However, this paper failed to reduce the computational overhead with the trade-off efficiency. Shen, et al [11]formed a Remote Data Possession Checking (RDPC) scheme for privacy preserving cloud data storage. In this environment, the Homomorphic Invisible Authenticator (HIA) was employed to securely protect the privacy of the user by constructing a Verifiably Encrypted Signature (VES). Also, the privacy of the authenticator was preserved by the use of remote data possession checking mechanism. The requirements that satisfied in this work were data correctness, soundness, authenticator privacy, and recovery. Moreover, the processes such as blockless verification, invisibility, and non-malleability were performed to ensure the security of the data storage. Cao, et al [12] designed a two-party preserving set intersection protocol for identifying and blocking the malicious users in cloud. Here, the functionalities of both commutative encryption and hash based commitments were incorporated for improving efficacy of the suggested protocol. The drawback behind this work was, it does not deploy the suggested protocol in an insecure infrastructure. Li, et al [13] developed a Lightweight Encryption mechanism for Database (L-EncDB)to preserve the data queries in cloud computing. Also, the Format Preservation Encryption (FPE) scheme was employed to encrypt the characters that stored in database. Moreover, the multi-radix modular addition was performed to preserve both the length and storage size of characters. In this framework, the ciphertext SQL by the use of trusted SQL interpretation layer. Then, it was further processed in the database layer with n number of fields. However, this work does not focus to implement the privacy preservation mechanism for data outsourcing. Shen, et al [14]formulated a Multi-dimensional Private Range Query (MPRQ) framework for enabling a secure data retrieval in cloud. The intention of this paper were to protect the access pattern, query and single dimensional privacy of the data. In this paper, a set of privacy requirements were established in a systematic way the outsourcing of encrypted cloud data. Also, the confidentiality of the data was protectedby implementing various policies. The advantage of this work was, it does not required any trusted third part for attaining the security in cloud. But, this paper has an increased computational overhead and time complexity, which were the drawbacks of this work.Jang, et al [15] designed a query integrity verification method for a secure data transfer in a cloud environment. Here, a query result authentication index was utilized to store the encrypted signature. Moreover, a bitmap data transformation technique was implemented to perform the cluster based data transformation. This architecture comprises the components of data owner, service provider, and trusted user. Also, the processes such as anchor selection with histogram, voroni based data clustering, and data transformation were performed. Moreover, a signature that used for generate a small group was constructed by using the condensed RSA technique. Zhu, et al [16] developed an Efficient Privacy Preserving Query (EPQ) scheme for a secure data outsourcing in cloud. In this paper, a Homomorphic encryption technique was utilized to enable a secure privacy preservation. Also, the Location Based Services (LBS) was executed with reduced computational overhead. This framework contains the following modules: system initialization, cloud server data creation, and privacy preservation. In this environment, the authenticated users were allowed to attain a desirable LBS data. The objectives that considered in this paper were, increased accuracy, guaranteed security requirements, efficient communication, and computation. The limitation behind this work was, it required to increase the trust level in the cloud server. Li, et al [17] employed a k-Nearest Neighbor (k-NN) algorithm for protecting the privacy of the data in cloud. Here, the kernel density was estimated by using a partially Homomorphic encryption technique. Moreover, the Data Owner – Queries (DO-Q) threat model was designed to detect the attacks based on distance learning. Also, the squared distances were computed based on the Gaussian kernel function. The suggested technique has an increased computational complexity, which was drawback of this work. Malina and Hajnv[18] suggested a privacy preserving solution for offering anonymous access to cloud services. Here, the operations such as bilinear pairing, modular exponentiation, and multiplication were performed. Also, the suggested solution satisfied the following requirements: anonymity, confidentiality, unlinkability, integrity, untraceability, and revocation. Moreover, the anonymous authentication was ensured and the user keys were protected against the collusion attacks. However, this paper required to reduce the impact of long size black list that used in the verification phase. Dili and Anu[19]maintained the integrity and security of the data stored in cloud. Here, the proxy re-encryption mechanism was utilized to satisfy the requirements of correctness, scalability, public auditing, and secure user revocation. In this system, the privacy was categorized into the forms of anonymity and unlinkability. Also, the integrity of the data was proved by revoking the user permanently. The advantages that observed from this paper were less communication resource, and preserved user's identity. At the same time, it required to reduce the communication cost and computation overhead. Chandran[20] designed a new model, namely, forward secure event oriented attributed based access control model for increasing the security of cloud. Here, the key generation was performed based on bilinear mapping, which includes the stages of Tsetup, Asetup, Usetup, AttrGen, and authentication. This work offered both unlinkability and linkability by using an event oriented access control. Yet, this paper failed to prove the effectiveness of the suggested system. Kaaniche and Laurent [21]examined various cryptographic mechanisms for providing privacy preservation and data security in cloud. In this study, the environmental threats, vulnerabilities, and risks were analyzed based on the cloud features. Also, the authors stated that the requirements such as public verification, stateless verification, low storage cost, low computational cost, and self-protect were must be satisfied for increasing the security. From this survey, it is observed that the existing techniques and frameworks have both benefits and demerits, but it mainly lacks with the following drawbacks:

- Reduced system efficacy
- High communication cost
- Increased computational complexity

To solve these problems, this paper aims to develop a new data outsourcing system for cloud.

3 PROPOSED SYSTEM

In this sector, the description about the proposed methodology is presented with its clear flow illustration. The intention of this paper is to securely outsource the data to a cloud server by analyzing the risks. The flow of the proposed Secure Crypto-based Data Outsourcing Model (SCDOM) is depicted in Fig 1. At first, the data owner collects the activity information of the participants presented in the smart environment. Then, those information are uploaded into the cloud server by the data owner. Once, the data user sends request to access the activity information, the cloud server forwards the encrypted data to the user. After that, the MAC is generated for the encrypted data. At the same time, the user also will generate the MAC key. This generated MAC by server and user are in turn forwarded to TPA. TPA will validate and verify the MAC keys for ensuring the integrity of the data access. Ifboth MAC Keys generationare valid, then data can be decrypted by obtaining the activity information from the cloud server; otherwise, the user will be blocked for further access.

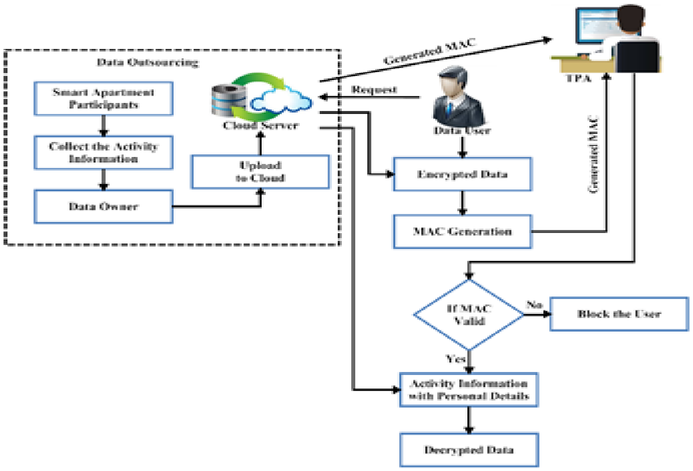

***Fig 2**. Flow of the proposed system*

3.1 Scope of the Proposed Methodology

The major contributions that focused in this work are listed as below:

Anonymity and Unlinkability

- Here, the data owner and the authorized agents can securely outsource the files to the remote cloud server.
- Then, the usage of complicated cryptographic key certificates is avoided by recognizing the participants of the users with their own attributes.
- Also, it proficiently supports to deploy the multi-user model in cloud.

Robust Widespread Auditing Model

- In this environment, the auditor verifies the integrity of the outsourced data in an efficient way.
- Then, the public common auditor is allowed to audit the files that owned by various users.

Low Communication Cost and Computation Complexity

- It uses the light weight methods for reducing the complexity in transmission time.
- The data communication is improved by increasing the power of sensor devices.

3.2 Encryption

Initially, the data user gives the request to the cloud server, then the server encrypts the data before transmitting it to the user. In this work, the blowfish encryption technique is utilized to encrypt the data, which is one of the widely used technique in cloud computing security. The blowfish is a kind of symmetric key cryptography technique that encrypts the 64 bit blocks with varying key length. The major benefits of using this technique are increased scalability, security, reduced execution time, and memory usage. Moreover, it contains two parts such as key generation part and data encryption part. In which, the secret key used for encrypting the data is considered as the identity attribute of the participant in the smart environment, which has the size of 128bits. The blowfish uses a large number of keys, which are pre-computed before data encryption.

Algorithm I – Key Generation and Data Encryption

```
//Key generation
Step 1: Let Key size be 128 bits or 16 Bytes
Step 2: $K_e$ (or) $IdP_{atr}$= identity Attribute of the participant.
Step 3: Let $K_l$= size ($IdP_{atr}$))
Step 4:  If $K_l$ >16
Step 5:         $K_e$= substring ($IdP_{atr}$, 16)
Step 6   Else if $K_l$ <16
Step 7:         $K_{Tl}$= 16 - $K_l$
Step 8:         For x= 1 to $K_{Tl}$
Step 9;                 $K_e$= $K_e$+x;
Step 10:                End for $K_{Tl}$
Step 11: End if $K_l$
//Encryption
Step 1: Let M=4, N=18
Step 2: Prepare $P_N$-array with N number of 32 bit sub keys from the input Key ($K_e$)
Step 3: Generate M number of S-boxes each of 256 bit size.
Step 4: Input plaint data is $D_{pl}$ may be of any size
Step 5: Convert the plaintext as a sub data of 64bit up to Size
        ($D_{pl}$)
Step 6: Now $Sub_{pl}\{L_{pl}, R_{pl}\} = D_{pl}$/2{32bit, 32 bit}
Step 7: For Y= 1 to 16 rounds
Step 8:  If Y<16
Step 9:         $L_{pl}$=$L_{pl}$⊕$P_Y$
Step 10:        $R_{pl}$=$R_{pl}$⊕$P_{Y+1}$
Step 11:        Increment Y
Step 12:        Swap ($L_{pl}, R_{pl}$);
Step 13:        Update P with S-boxes elements;
Step 14:Else If Y=16
Step 15:        $L_{pl}$=$L_{pl}$⊕$P_Y$
Step 16:        $R_{pl}$=$R_{pl}$⊕$P_{Y+1}$
Step 17:        Increment Y
Step 18:        Swap ($L_{pl}, R_{pl}$);
Step 19:        Update P with S-boxes elements;
Step 20:        $D_{en}$= merge {$L_{pl}, R_{pl}$}Step 21:      End if Y;
Step 22: End for Y;
```

3.3 MAC Generation and Verification

Once the user receives the data, the MAC for the encrypted data is generated by both user and server. In this stage, the hash is generated for the corresponding input key, based on this the 64-bit MAC is generated. The hash and MAC functions can support the incremental update property. The MAC is mainly used to validate the integrity of the data stored in cloud. Also, it ensures the confidentiality, and availability of the data based on the level of privacy. Typically, MAC is a fixed block of data that is generated based on the secret key, which is known as cryptographic checksum. It can be generated by the data user, owner and server by checking whether the data is altered or damaged during the transmission. Moreover, the pre-key and post-key are computed during this process by performing the XOR operation. After that, the generated MAC is validated by the TPA for verifying the integrity of the data. If both MAC are same, the data can be decrypted by the user by obtaining the activity information and personal details from the cloud server.

Algorithm II – MAC Generation

```
Step 1: Input Key for Generation of hash is =$K_e$ (or) $IdP_{atr}$
Step 2: Let $D_M$ = data for which Mac has to be generated.
Step 3: Hash function which is chosen is SHA-256 for which 64bit MAC will be generated
Step 4: Let block size ($Bx_S$) will be 32 bit
Key Generation:
Step5: $K_l$Be the Size of $IdP_{atr}$
Step 6:  If$K_l$>$Bx_S$)
Step 7:         $K_H$= hash ($IdP_{atr}$)
Step 8:  Else if $K_l$<$Bx_S$)
Step 9:         $K_H$= $bit_{pad}$($IdP_{atr}$, $Bx_S$)
Step 10: Else
Step 11: $K_H$=$IdP_{atr}$
Step 12: End if
Step 13: $Pre_{Key}$= $K_H$⊕(multiply (0x5c,$Bx_S$))
Step 14: $Post_{Key}$= $K_H$⊕(multiply (0x36,$Bx_S$))
Step 15: $d_{MAC}$= hash ($Pre_{Key}$,$D_M$)
Step 16: $d_{MAC}$= hash ($d_{MAC}$,$Post_{Key}$)
```

3.4 Data Decryption

After MAC verification, the encrypted data can be decrypted based on the user attribute. If the generated MAC are valid, the cloud server sends the activity information of the participant in the smart environment. The secret key is also generated in this stage based on the procedure that mentioned in the encryption algorithm. Then, the encrypted data is converted into the sub data with 64 bits.

```
Algorithm III – Decryption
Input: Encrypted Data, user Attribute as Key;
Output: Original plain text.
Step 1: Generate Key in the same pattern mentioned in the encryption module.
Then the encrypted data is decrypted by using the same set of S-boxes and $P_N$ array by applying the XOR operation in the $P_N$ in the reverse order.
Step 2:  Convert the encrypted data as a sub data of 64bit up to Size ($D_{en}$)
Step 3; Now $Sub_{en}\{L_{en}, R_{en}\} = D_{en}/2\{32bit, 32 bit\}$
Step 4: For Y= 16 to 1 round
Step 5:  If Y>16
Step 6:           $L_{en}=L_{en}\oplus P_Y$
Step 7:           $R_{en}=R_{en}\oplus P_{Y+1}$
Step 8:           Decrement Y
Step 9:           Swap ($L_{en}, R_{en}$);
Step 10:                Update P with S-boxes elements;
Step 11: Else If Y =1
Step 12:                $L_{en}=L_{en}\oplus P_Y$
Step 13:                $R_{en}=R_{en}\oplus P_{Y+1}$
Step 14:                Decrement Y
Step 15:          Swap ($L_{en}, R_{en}$);
Step 16:                Update P with S-boxes elements;
Step 17:                $D_{pl}$= merge {$L_{en}, R_{en}$}
Step 18: End if Y
Step 19: End for Y;
```

3.5 Data Anonymization

The data Anonymization is extensively performed to prevent the sensitivity of the owner's data, and to alleviate the unidentified risks. Usually, the privacy of the information is maintained by aggregating some information that are shared to the user. The major benefit of data Anonymization is increased security of the public cloud. During Anonymization, the set of participant attributes are given as the input, for instance, the age of the participant is considered in this process. If the age is greater than or equal to 50, the participants are categorized into type 1; otherwise, they are categorized into type 2. Similarly, other attributes such as capital gain, capital loss, occupation, and marital status are considered for Anonymization. In this paper, k-Anonymity is utilized. k- Anonymity: It is mainly used for screening or hiding the key information in a database of k-users. This approach will anonymise the quasi-identifiers and will provide privacy to the data. The major purpose of using k-anonymity is to make every record similar from other records. It deploys three types of data attributes as below, Key Attribute – It is used for identifying n number of individuals directly. Quasi – identifier – It will link with external information in order to identify the individual. Sensitive Attribute – It denoted the sensitive data to be exposed by an individual. K-Anonymity can be achieved through two ways. They are as below,

- Bottom Up Generalization
- Top Down Specialization

Bottom up Generalization: This strategy will initialize the data to its recent state and generalizations are being done until k-anonymity is not violated.

Top down Specialization: This strategy will initialize the data values to its base value of the hierarchy tree and the specializations are done iteratively until k-anonymity is violated.

```
Algorithm IV – Anonymizationusing K-anonymity
Input: set of Participant Attributes
Output: Anonymized Attributes
I ← age
N ← no of information
O ← Occupation
J ←  Anonymized age values
Tm ← 50
Step1:  For I← n
Step 2: if I < Tm
Step 3:  j ← j<Tm
Step 4: end if
Step 5: else
Step 6: j ←i>Tm
Step 6: end else
Step 7: End for
Step 8: Ik← 0
Step 10: th← 4
Step 8: for k to n
Step 11: s [ik] ← k
Step 12:  if  sk [ik] >th
Step 13: sk[ik]← *
Step 14: end if
Step 15: end for
```

4 PERFORMANCE ANALYSIS

In this sector, the experimental results of existing and proposed techniques are evaluated and compared by using various performance measures, which includes time consumption, memory consumption, communication overhead, encryption time, decryption time, computational cost, and execution time. Also, the existing techniques such as Shacham and Waters (SW), Anonymous Secure Framework (ASF), Identity Based Data Outsourcing (IBDO), Lightweight Secure Session Key Establishment (LSSKES) scheme, Device Authentication Mechanism (DAM), and Asymmetric Elliptic Curve Cryptography (AECC) are considered to prove the effectiveness of the proposed SCDOM technique.

4.1 Time Consumption

Response time is defined as the amount of time difference from the release time and the finishing time of a given task. Here, the response time is calculated for both existing and proposed techniques with respect to varying detection probability. It is calculated as follows:

$$Response\ time = Task\ receiving\ time - Task\ assigning\ time \tag{1}$$

In Fig 3, the value of the detection probability is varied from 0.5 to 0.99, based on this value, the time in terms of seconds is calculated. When compared to the existing[9]SW and IBDO, the proposed SCDOM provides the reduced time consumption.

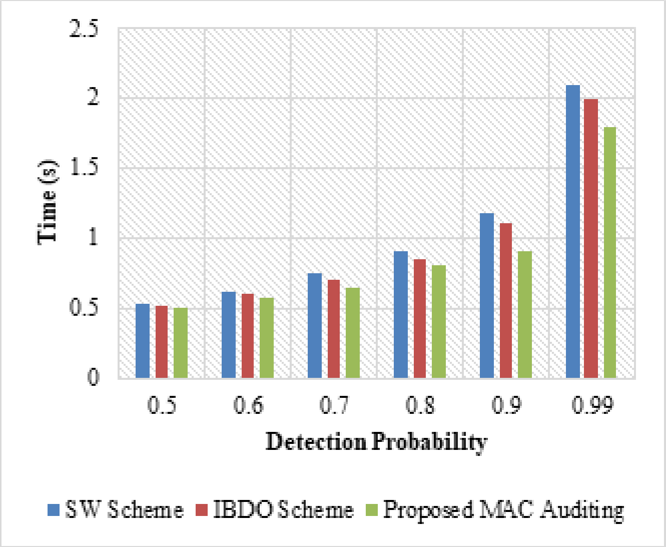

Fig 3. *Time consumption*

4.2 Communication Overhead

The communication overhead is estimated by the total number of transmitted and received bits by the device. Fig 4 shows the communication overhead of both existing [8] LSSKES, ASF and proposed SCDOM techniques with respect to the number of transmitted, received, and total bits. When compared to the existing techniques, the resultant communication overhead of the proposed method is reduced to 256 bits.

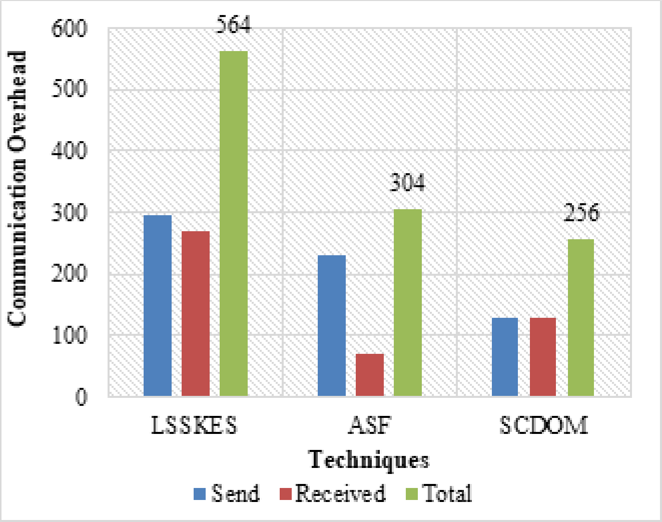

Fig 4. *Communication overhead*

4.3 Memory Consumption

Memory consumption is defined as the amount of memory that is utilized for data storage, and also it is defined as an occupied capacity of CPU. Fig 5 shows the memory consumption of both existing and proposed techniques with respect to the hash and encryption operations. From the analysis, it is evaluated that the proposed technique consumes less storage space for data storing, when compared to the existing ASF technique.

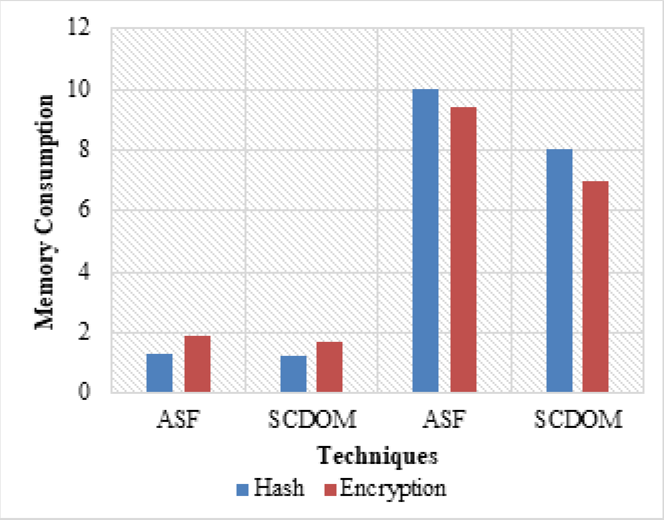

Fig 5. *Memory consumption*

4.4 Key Generation Time

Key generation time is defined as the amount of time that SCDOM taken for transferring the information and its execution. It is calculated as follows:

$$Key\ Generation\ Time = Information\ Transferring\ Time + Execution\ time \quad (4)$$

In this analysis, the key generation time of SCDOM is calculated with respect to varying number of data size and its graphical representations are shown in Fig 8. In this evaluation, it is proved that the proposed SCDOM requires the less key generation time by using the blowfish encryption algorithm.

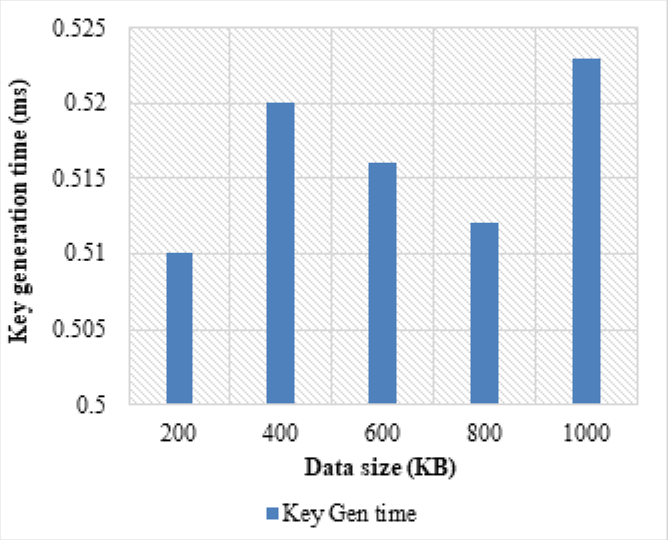

Fig 8*. Key generation time Vs Data size*

4.5 Execution Time

Execution time is defined as the amount of time required to execute the given process or job. Here, the execution time is calculated for the operations of hash, encryption, decryption, and XOR, which is shown in Fig 9.

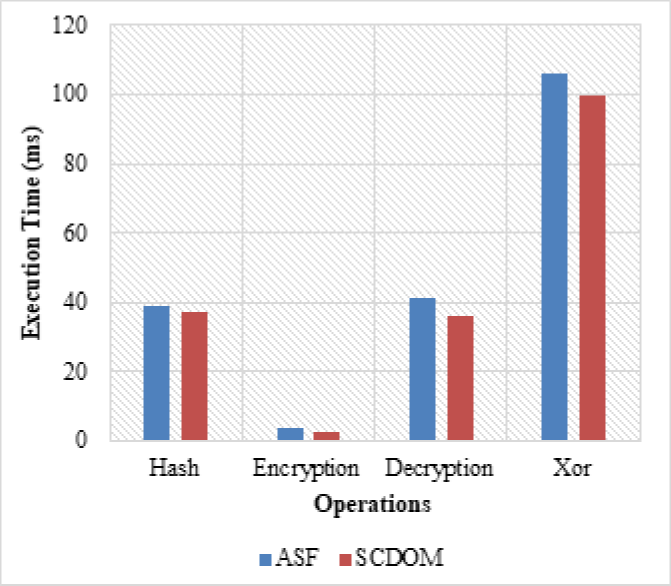

***Fig 9**. Execution time*

When compared to existing ASF technique, the proposed SCDOM requires the minimized execution time. It is calculated as follows:

$$Execution\ Time = Ending\ time\ of\ the\ process - Starting\ time\ of\ the\ process \quad (5)$$

Also, the total execution time of the existing and proposed methods are evaluated and illustrated in Table 1. In this evaluation, it is proved that the proposed SCDOM requires less total execution time, when compared to the other techniques.

TABLE 1

TOTAL EXECUTION TIME

Measure	DAM	AECC	LSSKES	ASF	SCDOM
Total Execution Time	~ 10.33	~10	~0.17	~0.12	~0.09

4.6 COMPUTATIONAL COST

The computational cost is fully depends on the measures of memory consumption and execution time. Here, the cost is evaluated for the Point Multiplication (PM), hash, MAC, HMAC, XOR, cryptosystem, and signature schemes, which is illustrated in Table 1. Here, the variable t represents the time for executing the point multiplication, H indicates the execution time of one way hash function, E denotes the encryption time, D denotes the decryption time, MAC is the time for performing the MAC operation, HMAC is the time for performing the HMAC operation, and XOR is the time for performing the XOR operation, and sig indicates the required time of signature generation. In this evaluation, the computation cost is evaluated for both existing DAM, LSSKES, AECC, ASF and proposed SCDOM techniques. From the evaluation, it is observed that the proposed SCDOM provides the anonymity and unlinkability by efficiently preserving the smart home devices with increased security and privacy.

TABLE 2

COMPUTATIONAL COST EVALUATION

Methods	DAM	LSSKES	AECC	ASF	SCDOM
PM	2t		2t		
Hash	4H	2H	1H	2H	
MAC		1 MAC			
HMAC		1 HMAC			1HMAC
XOR				3XOR	
Crypto		1E +1D		1E+1D	1E+1D
Sign	1 sig		1 sig		

5 CONCLUSION

In this work, a new SCDOM technique is proposed to securely outsource the data to the cloud server and to monitor the activities of the participants in the smart environment. Here, the smart apartment environment is considered, where the actions of all the members are monitored and controlled by employing a security mechanism. In this environment, the cloud server maintains the actions of all members, which is considered the highly trusted server. When, the user sends the request to the server, it encrypts the original data by using the blowfish encryption mechanism, then transmits it to the data user. The TPA has the responsibility to verify the trustiness of the user by validating the MAC generated by both the user and server. The user can be decrypt the data, only if the MAC is valid; otherwise, the user will be blocked for further access. The blowfish technique is also used to decrypt the data based on the activity information and personal details attained from the server. The major merits of this system are increased security, reduced complexity, and time consumption. Also, it avoids the exchange of complicated cryptographic key certificates by recognizing the participants of the cloud with their own attributes. During the experimentation, the results of the existing and proposed SCDOM are evaluated and analyzed by using various performance measures. From the investigation, it is observed that the proposed SCDOM provides an efficient results, when compared to the traditional techniques. In future, this work can be enhanced by implementing this mechanism in a real time applications such as health care, and smart city.

REFERENCES

[1] Y. Yu, M. H. Au, G. Ateniese, X. Huang, W. Susilo, Y. Dai, et al., "Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage," IEEE Transactions on Information Forensics and Security, vol. 12, pp. 767-778, 2016.

[2] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. S. Shen, "Security and privacy in smart city applications: Challenges and solutions," IEEE Communications Magazine, vol. 55, pp. 122-129, 2017.

[3] "http://image.ntua.gr/iva/datasets/ec1m/."

[4] U. Gupta, M. S. Saluja, and M. T. Tiwari, "Enhancement of Cloud Security and removal of anti-patterns using multilevel encryption algorithms," 2018.

[5] A. Choudhury, B. Roy, and S. K. Misra, "Data Integrity and Compression in Cloud Computing," International Journal of Computer Applications, vol. 168, 2017.

[6] S. Chaudhari and S. K. Pathuri, "A Comprehensive Survey on Public Auditing for Secure Cloud Storage," International Journal of Engineering & Technology, vol. 7, pp. 565-569, 2018.

[7] A. Jacobsson, M. Boldt, and B. Carlsson, "A risk analysis of a smart home automation system," Future Generation Computer Systems, vol. 56, pp. 719-733, 2016.

[8] P. Kumar, A. Braeken, A. Gurtov, J. Iinatti, and P. H. Ha, "Anonymous Secure Framework in Connected Smart Home Environments," IEEE Transactions on Information Forensics and Security, vol. 12, pp. 968-979, 2017.

[9] Y. Wang, Q. Wu, B. Qin, W. Shi, R. H. Deng, and J. Hu, "Identity-based data outsourcing with comprehensive auditing in clouds," IEEE Transactions on Information Forensics and Security, vol. 12, pp. 940-952, 2017.

[10] A. Alabdulatif, H. Kumarage, I. Khalil, and X. Yi, "Privacy-preserving anomaly detection in cloud with lightweight homomorphic encryption," Journal of Computer and System Sciences, 2017.

[11] W. Shen, G. Yang, J. Yu, H. Zhang, F. Kong, and R. Hao, "Remote data possession checking with privacy-preserving authenticators for cloud storage," Future Generation Computer Systems, 2017.

[12] X. Cao, H. Li, L. Dang, and Y. Lin, "A two-party privacy preserving set intersection protocol against malicious users in cloud computing," Computer Standards & Interfaces, vol. 54, pp. 41-45, 2017.

[13] J. Li, Z. Liu, X. Chen, F. Xhafa, X. Tan, and D. S. Wong, "L-EncDB: A lightweight framework for privacy-preserving data queries in cloud computing," Knowledge-Based Systems, vol. 79, pp. 18-26, 2015.

[14] Y. Shen, W. Yang, L. Li, and L. Huang, "Achieving fully privacy-preserving private range queries over outsourced cloud data," Pervasive and Mobile Computing, vol. 39, pp. 36-51, 2017.

[15] M. Jang, M. Yoon, and J.-W. Chang, "A New Query Integrity Verification Method with Cluster-based Data Transformation in Cloud Computing Environment," International Journal of Smart Home, vol. 9, pp. 225-238, 2015.

[16] H. Zhu, R. Lu, C. Huang, L. Chen, and H. Li, "An Efficient Privacy-Preserving Location-Based Services Query Scheme in Outsourced Cloud," IEEE Transactions on Vehicular Technology, vol. 65, pp. 7729-7739, 2016.

[17] F. Li, R. Shin, and V. Paxson, "Exploring privacy preservation in outsourced k-nearest neighbors with multiple data owners," in Proceedings of the 2015 ACM Workshop on Cloud Computing Security Workshop, 2015, pp. 53-64.

[18] L. Malina and J. Hajny, "Efficient security solution for privacy-preserving cloud services," in Telecommunications and Signal Processing (TSP), 2013 36th International Conference on, 2013, pp. 23-27.

[19] G. Dili and V. Anu, "Maintaining Integrity and Security for the Data Shared in the Cloud," International Journal of Engineering Science, vol. 7693, 2016.

[20] M. M. Chandran, "Forward Secure Event Oriented Attribute based Anonymous Access Control for Cloud Computing," International Journal of Computational Intelligence Research, vol. 12, pp. 223-226, 2016.

[21] N. Kaaniche and M. Laurent, "Data security and privacy preservation in cloud storage environments based on cryptographic mechanisms," Computer Communications, vol. 111, pp. 120-141, 2017/10/01/ 2017.