ION EXCHANGE AND ADSORPTION
ISSN: 1001-5493
Vol. 23, Issue-01, 2023
pp.241-247

MULTILEVEL ENCRYPTION WITH MULTIPLE-CLOUD STORAGE (MEMC) WITH BOT DETECTION AND ELIMINATION (BDE) IN RECOMMENDATION SYSTEM

J Chitra
Research Scholar-Vistas

Dr. SK. Piramu Preethika
Assistant Professor, Vistas

ABSTRACT

In general cloud acts as an intermediate in Publish and Subscribe (pub/sub) system to broadcast the publisher's data to the subscribers. But a direct connection among the subscriber and the publisher is not advisable only a loosely coupled manner allowed along with the cloud. There lot of chances in data getting exposed to the attackers from the client side, publisher side or even from the cloud side. Attackers, specifically botnet controllers, use stealthy commanding systems to set up large-scale control. Encryption before upload is the best way of protecting a sensitive publications and subscriptions. In the proposed system a novel mechanism named as "Multilevel Encryption with multiple-cloud Storage (MEMC) with BOT detection and elimination (BDE)" is produced. The proposed mechanism is used to secure the publications and subscriptions by providing a multilevel encryption technique before it is disseminated to the cloud. To tackle the un-trusted cloud the system provides an Epub/Esub an encryption system of both to maintain the confidentiality. Further As, the BOT type attacks are common in cloud to resist and overcome this system introduces a BOT detection and elimination technique. Finally, the experimental results ensure the efficiency, performance and feasibility of the system.

Keywords- multi-level encryption, Secure Pub/sub, Subscribers' security, Publications' Confidentiality, BOT attack.

I. INTRODUCTION

Commonly cloud acts as a supporting storage unit that stores enormous user data and the publisher data. At times there are chances that the user data or the publisher sensitive data may be misused or hacked by multiple attacks. Even cloud may get compromised for exposing the sensitive data to the malicious entities. Hence, there is no guarantee for a data when it reaches a public commodity. Simultaneously, pub and sub system work in the very similar way that the data from the publications are recommended according to the interested subscribers in a loosely-coupled way. The main form of transmission in this Publish and Subscribe (pub/sub) system is accelerated through recommendation. In general the data created by the publishers are represented as publications these publications are referred to the interested subscribers via servers called as cloud. The cloud services providers offers cloud services as Software as a Service (SaaS) to the entire network. Basically, publication content is defined with a set of tags with a keyword extraction. Accordingly considering the set of constraints on these tags the interested subscriptions are made by the subscribers. To appraise the interest of the subscribers in particular publication the set of tags are matched with interests registered by the subscribers. By identifying interest for the specific publication stored in the server, the publication id

directed to the intended subscribers automatically. The proposed work deliberates an extension of the preceding work [1] that emphasizes privacy over in Publish and Subscribe Systems. The publish and subscribe system is used widely in several applications such as health-care, marketing, stock exchange, book or article publishing etc.,[2-4]. Google, which is the real-time messaging service, offers the pub and sub system for analytics and computing systems (event-driven). Accounting the benefits of pub and sub system the demerits and challenges cannot be ignored that cause major impact on privacy of data by a set of cloud. Accounting the outsourcing unit, the pub/sub service relies on the cloud servers which can be compromised easily. Unfortunately these cloud servers cannot be trusted in 2016 the yahoo attack caused leakage of 1 billion accounts leading to privacy issues [7]. To secure the publication and subscription from the un-trusted entities and to handle the sensitive data some preventive measure and methods are used in the paper. The privacy protection method and attack prevention techniques are multi-fold deliberated as follows:

- Initially in this paper privacy preserving publish and subscribe system protecting both the publication s and subscription personal details and identities are proposed. The multiple cloud storage compromising the pub and sub system is broken by following a high multi-level encryption technique. The formation of multi-level encryption using multiple cloud storage (MEMC) together forms a new model.
- A 'Searchable Encryption (SE)' technique is followed to assure encrypted publication keyword matching beside the interest of subscribers. The system efficiency relies in using multiple cloud storage for matching and routing the trustable publication to the trustworthy interested subscriber. The ideal thought is to split the match operation to several phases along with encrypted subscriptions and publication tags. Each and every phase is assigned for different cloud server for privacy maintenance.
- The partitioned data will be processed by different type of cloud servers to avoid the sensitive data a leak. Even if the one particular cloud server is compromised and colludes with a subscriber or a publisher for data leak it will not affect any data privacy the subscriptions and the publications are still protected.
- Further, to identify and stop the BOT controlling the system introduced 'BOT detection and Elimination (BDE)' model.

The rest of the paper is organised as follows. Section 2 describes the requirement for secure access. Sections 3 possess a discussion on surveys related to previous work. Entering section 4 both the proposed system model and the threat model are discussed together. Section 5 provides an experimental security analysis with comparative analysis. Finally, the paper is concluded in Section 6 highlighting some future research directions.

II. SECURITY REQUIREMENTS

In order to ensure a secure privacy-preserving pub/sub service, the network must maintain the privacy of each publications and confidentiality of subscriptions. Also a proper secured encrypted recommendation is very important.

The publicized data should be protected against the cloud servers and unauthorised subscribers/publishers. The publishers and subscribers should not communicate directly they must be loosely coupled. For instance, consider a health care management the publications or data must be in form that it should be accessed only by the cloud server that matches publications' tags of authorised subscribers. The subscribers that do not match the publications' tags are not allowed to access the information of the publishers. The cloud is designed in a way that it checks for an authorized subscribers, trusted publishers and mainly checks for the publication tags matching with the interest of the subscribers. The identity or locations of the publishers/subscribers are hidden even if the matches are identified.
Also, the system should be capable of identifying any attacks. It should mainly identify and stop BOT controls.

III. LITERATURE REVIEW

Some of the existing methodologies researched by the authors are discussed for a proper pub and sub management.
W.Rao et al., in [8] produced a mechanism correlating subscribers and cloud servers possessing a secure pub/sub system. A system resisting collusion attacks among the un-trusted subscribers (or publishers) and cloud server are discussed in previous approaches in [9,10]. The system processes a direct communication for publishers and subscribers privacy against colluding parties. A secure broker less publish/subscribe system projected by Tariq et al., where the publication is processed by a trustable publishers. For encryption the system uses CPABE Ciphertext-Policy Attribute-Based Encryption method in [11]. Also a public-key encryption technique followed in processing keyword search [12].
F. Hahn and F. Kerschbaum [13] projected a new scheme named as SUISE symmetric Searchable Encryption that process encryption by interests and tags and acknowledges a secures encrypted subscription.
Y. Polyakov et al., [14] stated a secured topic related publish/subscribe system related to proxy encrypting technique. Further the author applied a lattice proxy encrypting scheme projecting a homomorphism operation with loosely coupled property of publish or subscribe system.
Pires et al. [15] currently introduce a routing engine offered by SGX enclaves for pub/sub system leveraging a trustable execution.

IV. METHOD IMPLEMENTATION

The proposed approach implementation with two divisions system Approach and the threat approach. Then, an extended overview of the method implementation is processed.

4.1 System Approach

A privacy-preserving pub/sub service mode is executed following the below steps:
The system model undergoes several sections pub section for publications, Sub section for subscriptions, cloud server (A,B,C) and trustable authority.

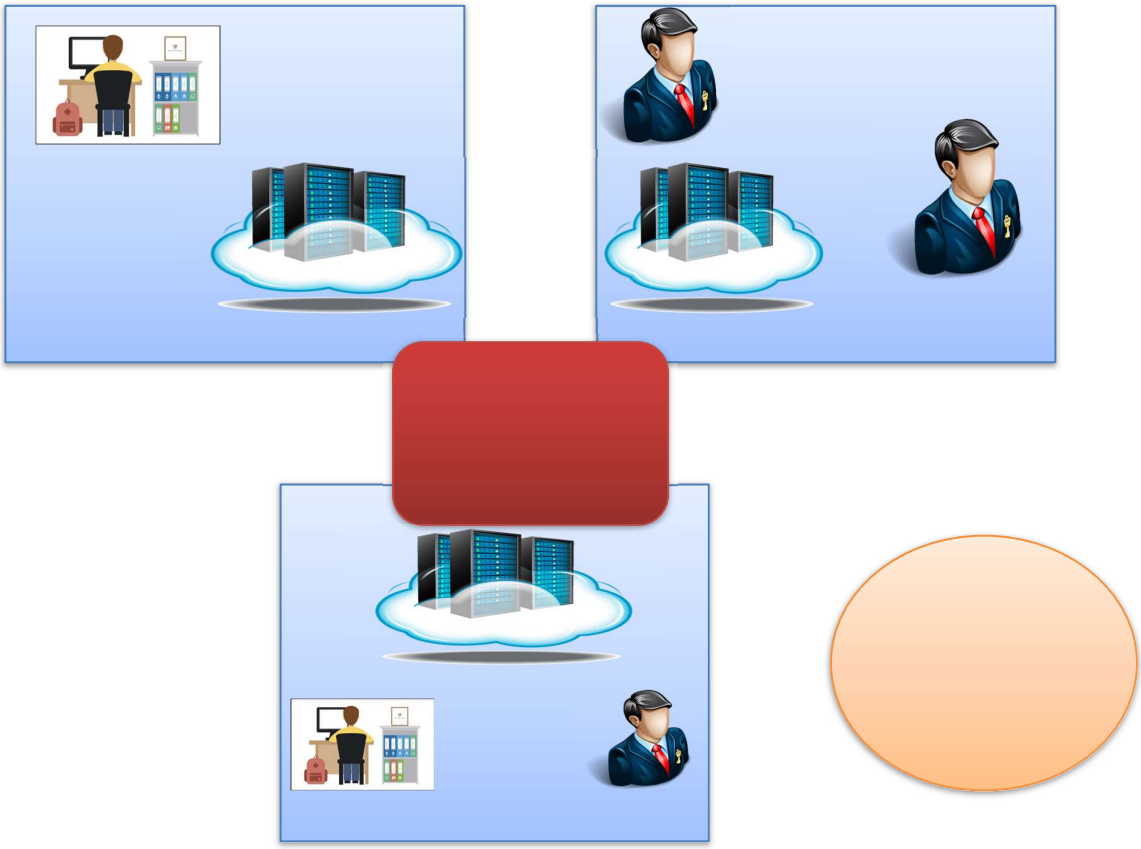


Figure 1. system architecture for proposed Pub/sub system model.

- *Encrypted Pub (Publishers) section*: In this section the publisher creates publications with their respective tags. For the publisher a specific cloud server is assigned before storing the publication both the payload and tag of publication are encrypted.
- *Encrypted Sub (Subscribers) section:* In Sub section the interest of the subscribers are collected and an encrypted subscriptions are made according to their interests. Only the publications that satisfy the subscription tags are recommended to the subscribers.
- *Cloud server*: for each section a separate cloud server is allotted. In the system 3 different type cloud server is assigned cloud A for subscriptions, cloud B for encryption and transferring, Cloud C for publications. The cloud server performs the filtration and delivering of publications according to the subscribers' interest.
- *Trustable encrypted Authority:* this section handles the key authorization to manage the subs/pubs system keys.

The above figure 1. provides a detailed system approach with the proposed implementation design. A publish/subscribe service providing protection to the publications and Subs' from the curious cloud server and malicious pubs and subs are provided.

4.2 EMC with SE Implementation:

A new approach named as 'Multilevel Encryption with multiple-cloud Storage (MEMC) proposed to handle the pubs/subs system. The encryption method is upgrade by multilevel

implementation. The data is encrypted at multiple stages and multiple times before performing any upload or storage. Initially the publisher uploads the publication to cloud A the system immediately encrypts the publications before uploading to the server. Cloud B is assigned for handling the encrypted subscriptions according to the subscriber interest. A searchable encryption technique is followed for recommending publications according to the subscribers' interest in the recommendation system.

4.3 Handling Threat Model

The general threat models are malicious Sub, malicious Pub, semi-trusted cloud server. A malicious sub tries to intrude through the unauthorized publications and interrupt other subs combining with cloud servers. A malicious Pub tries to interfere in subscribers' interest by intrusion with some malicious publications along with servers. Some servers are not trustable. Though they follow the rules of the subscription they interfere in the publication content and interest of the subscriber.

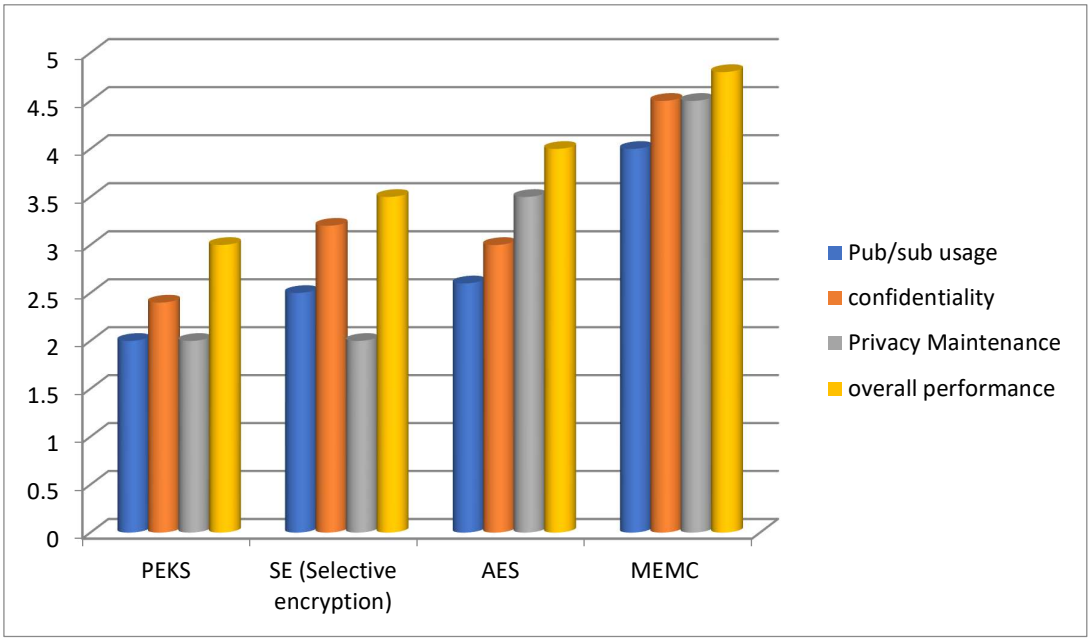
The above mentioned threat model can be handled by following a set of encryption protocols. A cloud server must contain capacity to handle at least three various non-colluding Domains.

4.4 BOT CONTROLLER for Detection and Elimination:

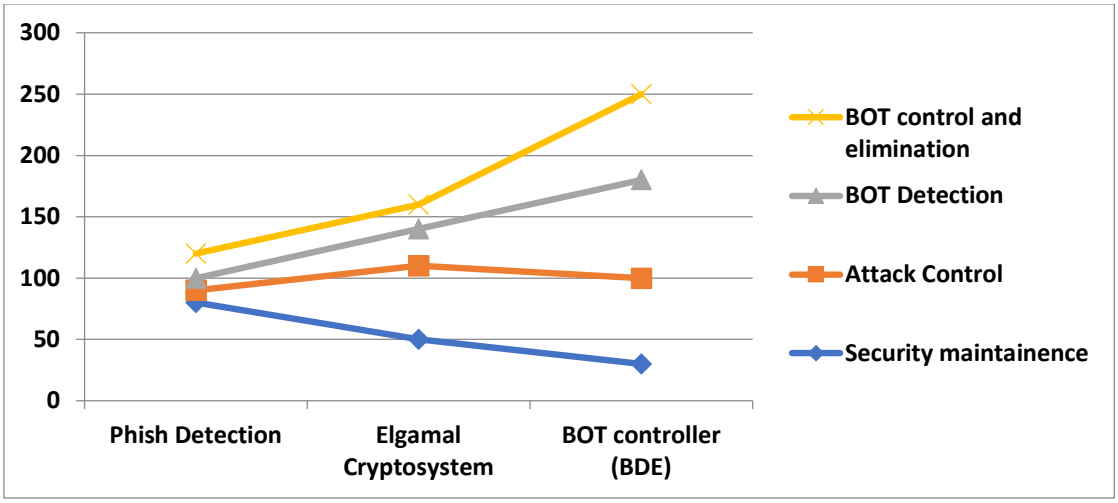
BOTS are automated systems that have access to command any type of data stored in cloud. Some curious BOTs collects data from the server unknowingly and takes control of subscriber and publisher data. To detect BOTs a BOT tracker is used where the BOT commands are tracked and eliminated immediately before any massive intrusion.

V. RESULTS ANALYSIS

In result analysis, a comparison of all the existing algorithms with the proposed model is done. A comparison of existing algorithms such as PEKS, Advanced Encryption System (AES), Selective encryption (SE) with the proposed model 'MEMC Multi-level encryption is using multiple storage' is made. The proposed models are more sustainable and effective in cloud data storage and user data security.



Graph 1. Comparitive Analysis of Proposed system vs Existing system



Graph 2. Comparing the encryption techniques

In the above graph deliberates the security enhancement chart with comparing the previous attack detection systems Elgamal cryptosystem and phish detection with the proposed system BOT controller (BDE) determined. The proposed HSD BDE is proved to have high privacy, execution promptness and attack elimination.

VI. CONCLUSION

In the proposed work, the cloud servers are partitioned and assigned for handling each work . the server is setup to follow a trustable protocol with proposing a trustable algorithm. A Multilevel Encryption with multiple-cloud Storage is projected for providing privacy over the pub/sub systems. Also, a proper recommendation system is handled for recommending the

accurate encrypted publication to the encrypted subscribers. Further, the system provides an attack detection mechanism with BOT controller provides detection and elimination of BOTs. As future work, the system will be designed to perform more complex encryption and some attack elimination algorithms can be used.

REFERENCES

[1] S. Cui, S. Belguith, P. De Alwis, M. R. Asghar and G. Russello, "Collusion Defender: Preserving Subscribers' Privacy in Publish and Subscribe Systems," in *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 3, pp. 1051-1064, 1 May-June 2021, doi: 10.1109/TDSC.2019.2898827.

[2] C. Esposito, M. Ciampi, and G. De Pietro, "An event-based notification approach for the delivery of patient medical information," Information Systems, vol. 39, pp. 22–44, 2014.

[3] M. Cinque, C. Di Martino, and C. Esposito, "On data dissemination for large-scale complex critical infrastructures," Computer Networks, vol. 56, no. 4, pp. 1215–1235, 2012.

[4] I. M. Delamer and J. L. M. Lastra, "Service-oriented architecturefor distributed publish/subscribe middleware in electronics production," IEEE Transactions on Industrial Informatics, vol. 2, no. 4, pp. 281–294, 2006.

[5] "Google cloud pub/sub," https://cloud.google.com/pubsub, last accessed: November 27, 2018.

[7] "Yahoo data breach," https://www.theguardian.com/technology/2016/ dec/14/yahoo-hack-security-of-one-billion-accounts-breached, 2016, last accessed: November 27, 2018.

[8] W. Rao, L. Chen, and S. Tarkoma, "Toward efficient filter privacy-aware content-based pub/sub systems," IEEE Transactions on Knowledge and Data Engineering, vol. 25, no. 11, pp. 2644–2657, 2013.

[9] E. Onica, P. Felber, H. Mercier, and E. Rivi`ere, "Confidentialitypreserving publish/subscribe: A survey," ACM Computing Surveys (CSUR), vol. 49, no. 2, p. 27, 2016.

[10] W. Rao, L. Chen, M. Yuan, S. Tarkoma, and H. Mei, "Subscription privacy protection in topic-based pub/sub," in International Conference on Database Systems for Advanced Applications. Springer, 2013, pp. 361–376.

[11] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," in S&P 2007. IEEE Computer Society, 2007, pp.321–334.

[12] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in EUROCRYPT 2004, ser. LectureNotes in Computer Science, C. Cachin and J. Camenisch, Eds., vol.3027. Springer, 2004, pp. 506–522.

[13] F. Hahn and F. Kerschbaum, "Searchable encryption with secure and efficient updates," in SIGSAC 2014. ACM, 2014, pp. 310–320.

[14] C. Borcea, Y. Polyakov, K. Rohloff, G. Ryan et al., "PICADOR: Endto-end encrypted publish–subscribe information distribution with proxy re-encryption," Future Generation Computer Systems, vol. 71, pp. 177– 191, 2017.

[15] R. Pires, M. Pasin, P. Felber, and C. Fetzer, "Secure content-based routing using Intel Software Guard Extensions," in Middleware 2016. ACM, 2016, p. 10.