Journal of ISMAC (2021)
Vol.03/ No.03
Pages: 250-262
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2021.3.006

Secure Data Sharing Platform for Portable Social Networks with Power Saving Operation

Jennifer S. Raj
Professor, Department of ECE, Gnanamani College of Technology, Namakkal, India.
E-mail: jennifer.raj@gmail.com

Abstract: Several subscribing and content sharing services are largely personalized with the growing use of mobile social media technology. The end user privacy in terms of social relationships, interests and identities as well as shared content confidentiality are some of the privacy concerns in such services. The content is provided with fine-grained access control with the help of attribute-based encryption (ABE) in existing work. Decryption of privacy preserving content suffers high consumption of energy and data leakage to unauthorized people is faced when mobile social networks share privacy preserving data. In the mobile social networks, a secure proxy decryption model with enhanced publishing and subscribing scheme is presented in this paper as a solution to the aforementioned issues. The user credentials and data confidentiality are protected by access control techniques that work on privacy preserving in a self-contained manner. Keyword search based public-key encryption with ciphertext policy attribute-based encryption is used in this model. At the end users, ciphertext decryption is performed to reduce the energy consumption by the secure proxy decryption scheme. The effectiveness and efficiency of the privacy preservation model is observed from the experimental results.

Keywords: Proxy Decryption; Ciphertext Decryption; Attribute-based Encryption; Privacy Preserving; Data Confidentiality

1. Introduction

User generated data is shared and subscribed over social networking platform by numerous internet users with the growing popularity and utilization of the internet [1]. Subscribing and sharing of content are the extremely popular services in online social networks

ISSN: 2582-1369 (online)
Submitted: 15.06.2021
Revised: 02.08.2021
Accepted: 18.08.2021
Published: 27.08.2021

Journal of ISMAC (2021)
Vol.03/ No.03
Pages: 250-262
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2021.3.006

that can be performed in a convenient manner with the mobile devices and their pervasiveness [2]. Interests, identities and other credentials of the users are used for subscribing to interested content or sharing own content by the users [3]. Netflix or YouTube is used for sharing and subscribing to videos while Photobucket or Flickr is used for sharing photos by millions of everyday users. Foursquare and other internet service providers are used for uploading the user credentials and for content sharing [4]. Close friends, family members and other eligible receivers can access the contents shared by the users. The social relationships, interests, identities and other sensitive user information may be accessed by the adversaries imposing serious threat to the user privacy while implementing certain target-sharing techniques. Private data of the users may be accessed and sold to advertisers without the permission of the user by malicious service providers [5].

Information leak has been observed in 20 of 30 popular android application on 68 instances by researchers [6]. Without permission or notification, the analytical servers and advertisers are provided with user information by 15 applications. The privacy of users is threatened by the sensitive data obtained from the service providers by attackers and unauthorized users [7]. Improper sharing and access of several private photos is done using the fusking technique from a prominent photo-sharing site bypassing the security settings by hackers according to the CNN report. The internet address of the user is exposed to the whole world by Skype according to The Wall Street Journal report [8]. The internet addresses may be linked to the Skype user account name using several malicious tools. Access to sensitive data is obtained from other users and service providers by unauthorized users [9]. The danger of data breach is also observed in the security hole of Google Drive. Users' data can be accessed with the leaked clickable URL from the service provider without the permission of the users.

In mobile social networks, the content sharing scheme with a privacy-preserving model is indispensable [10]. The content can be retrieved through fine-grained access control with the help of an attribute-based encryption (ABE) technique. Based on the content accessing authority, be it the key generation authority (KGA) or publisher, key-policy ABE (KP-ABE) and ciphertext-policy ABE (CP-ABE), two ABE schemes are obtained. The service provider is exposed to the sensitive access policy due to new privacy concerns faced by the original ABE scheme [11]. A combination of keyword search and public-key encryption is used to

ISSN: 2582-1369 (online)
Submitted: 15.06.2021
Revised: 02.08.2021
Accepted: 18.08.2021
Published: 27.08.2021

Journal of ISMAC (2021)
Vol.03/ No.03
Pages: 250-262
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2021.3.006

address this issue in the ABE scheme. Without data regarding the credentials of the user, access policy and shared content, matching is performed by the service provider using this modified algorithm [12]. At the end-receiver, high energy consumption is observed as the end-receivers are distributed with the decryption task for several applications by this combination of ABE, of keyword search and public-key encryption. The decryption time and ciphertext size is directly proportional to the size and complexity of the access policy. Energy efficiency is a prominent challenge of all the issues faced by this modified ABE technique [13-15].

An efficient and effective model ensuring user privacy based on an autonomous privacy preserving data sharing model is essential to overcome the aforementioned concerns [16]. A secure proxy decryption scheme with a publish-subscribe model is proposed in this paper that does not impose the authorized subscribers with energy-intensive computational complexity while maintaining the subscriber and publisher privacy as well as the shared content confidentiality. The content publisher indicates certain access policy that must be matched by the credentials provided by the authorized users for content sharing. No access is provided to the shared content for unauthorized viewers concerning shared content [17]. Without learning the subscriber credentials or the publisher's private information is not shared while sharing the encrypted content with authorized users by the service providers. Content is recovered by using exponentiation operation on the partially decrypted ciphertext and it's constant size by authorized users.

2. Literature Review

The publish-subscribe model and other entities such as security challenges and threat model in the content sharing services currently available are studied. Content is generated and shared with specific users by the publisher [18]. The interests of the subscriber is uploaded to the service provider for subscribing to specific interests. The authorized subscriber is provided with the content after matching the uploaded content to the interest of the subscriber. KGA, a trustworthy third-party application is used for generating private as well as public user keys. An out of band pattern is observed during the delivery of all the keys. At the user's initialized phase, allocation of keys is performed in general. Certain significant aspects are noted while describing the threat model. Honest and curious nature of the service provider is a primary

ISSN: 2582-1369 (online)
Submitted: 15.06.2021
Revised: 02.08.2021
Accepted: 18.08.2021
Published: 27.08.2021

Journal of ISMAC (2021)
Vol.03/ No.03
Pages: 250-262
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2021.3.006

assumption [19]. A sharing scheme is used for specifying operations that are executed honestly. However, the maximum extent of sensitive information is extracted from the user. Sensitive data may be obtained by malicious users that colludes with the service provider. In order to obtain critical data, collusion between malicious users may also occur. Deliberate discarding or intercepting of transferred data is not considered in these scenarios [20].

To provide privacy protection and efficient process, for publishing, service providing and subscribing certain challenges must be considered, they are how to ensure that unlicensed audiences does not get access to the contents that were shared, the publisher specifies certain access policies and it should not recognize to unlicensed user and service provider, when benefits and characteristics of the subscribers are not known, how the content will be shared by the service provider, ensure that the licensed subscribers receives only encrypted contents for minimizing the bandwidth overhead, ensuring that there should not be any complexity in exempting the computational difficulty in decrypting the data [21]. The secrecy preserving of location development and secrecy preserving of location based on block-chain is discussed and certain encrypting algorithms are to be discussed [22].

The sharing of location by the users to the requesters of location has to be preserved and the methods involved in preserving the locations are false location, cryptography, differential privacy and k- anonymity. For understanding the location privacy preserving the false location is returned and in mobile devices, it is not suitable and as it retains high cost, so that Bayesian games is utilized [23]. For reducing the system overhead, DA is an effective method which enlightens the energy efficiency and decreases the bandwidth occupation. When there emerge many attacks in the network, the uncertain positioning pattern and broadcast mode of communication makes DA a challengeable one. To provide guarantee to confidentiality of sensing data the DA method with some privacy preserving protocols is to be proposed. SMART (Slice-Mix-AggRegaTe) includes three steps and it includes DA privacy preserving. In SMART method the sensed data is divided into different parts and divided slices are sent to different destination points for hiding the confidential information in different slices. Also, this method was proven by many researchers as a method that provides low cost in communication bandwidth [24]. mOSNs have developed rapidly after increasing use of mobile devices, the main convenience for people is location sharing but there are also certain issues in

ISSN: 2582-1369 (online)
Submitted: 15.06.2021
Revised: 02.08.2021
Accepted: 18.08.2021
Published: 27.08.2021

Journal of ISMAC (2021)
Vol.03/ No.03
Pages: 250-262
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2021.3.006

considering it. For addressing this kind of issues, many methods have been developed namely, k-anonymity [25], spatial cloaking [26] and dummy [27]. In location sharing environment the efficiency of the system and security are two factors that is to be considered. For the protection of confidential data like locations and identities many different methods was proposed, during the process of sharing the location, the identities of the user may be seeped to the server hence MobiShare+ was proposed that protects the privacy of the identity by employing dummy queries [28]. A broadcast method was used for requesting the data of friends in the neighbourhood and developed a cryptography method known as functional pseudonym for protecting the identity information of the user [29]. For the privacy issue that are caused due to location information a method was proposed “A game-theoretic framework”, it discovers the association between user location and their behaviour [30].

In the system of location sharing, there is a possibility of providing the imprecise positioning hence an attack method was developed for disclosing the faults of protective location confidentiality in sharing of location method [31]. A secure distance comparison procedure was proposed for preventing the revelation of identities of users that are due to threshold detachments. All these solutions concentrate on the security necessities in sharing of location but the user defined privacy preserving necessities cannot be met. A user defined access control strategy was developed for battling the attacks from neighbourhood and it permits the user to regulate whether the location is to be shared with friends. This is suitable for some of the trust less friends but not in case of confidential areas. If some privacy preserving necessities is handled by the user, in certain areas such as workplace, the access control strategy must be set by the user each and every time to all of his friends. In the same way when the user needs to use the sharing of location process, when they move to different places, they have to reorganize the access control strategy. This method will not be flexible when privacy preserving necessities are needed in confidential areas [32]. Some methods needed to be proposed for progressing the efficiency when user privacy is to be maintained. In order to reduce the time needed for finding the location of the user and improve the efficiency of the search, the location update database must be developed but this method is a burden for storage. B- Mobishare scheme was used for increasing the efficiency of the transmission and for filtering the confidential data that is to be transmitted between server of social network and

ISSN: 2582-1369 (online)
Submitted: 15.06.2021
Revised: 02.08.2021
Accepted: 18.08.2021
Published: 27.08.2021

Journal of ISMAC (2021)
Vol.03/ No.03
Pages: 250-262
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2021.3.006

location, a bloom filter method should be used, but it leads to computational overhead and high time cost [33].

3. Proposed Method

A content sharing scenario is presented first, then a privacy preserving method is presented next in an advanced way. Assume a situation in a marketable environment, where a memo wants to be shared by the board of directors in a company to some specific persons, which gratify organizational levels through the cloud service provider. The memo is labelled by the publisher with a tag trade. By uploading the characteristics and benefits by the mobile or computer devices, to the cloud service provider, the attentive document can be subscribed by the persons. By using the access policy, the memo will be encrypted. Only if the authorizations satisfy the policies, the memo can be received by the subscriber. The access policy can be labelled with a tree, where the leaf node comprises attributes, AND, OR or threshold gates are composed in non-leaf nodes. Considering that the manager or director can only access the memo, and the access policy can be illustrated by a tree as shown in Figure 1.

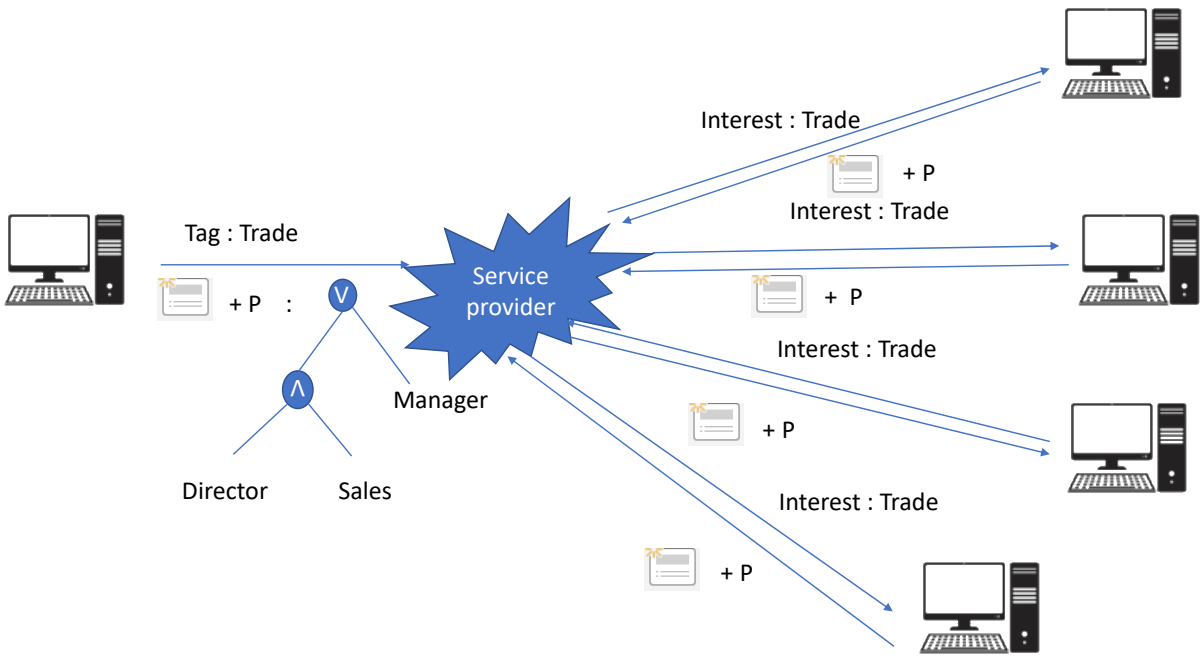

Figure 1. Attribute based Broadcast Encryption Method

ISSN: 2582-1369 (online)
Submitted: 15.06.2021
Revised: 02.08.2021
Accepted: 18.08.2021
Published: 27.08.2021

Journal of ISMAC (2021)
Vol.03/ No.03
Pages: 250-262
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2021.3.006

Scheme 1: Attribute Based Broadcast Encryption: The shared content is encrypted by an access tree for maintaining the privacy of it, and then for distinguishing the shared contents from other contents, they are labelled with a tag. The service provider is provided with the content that is encrypted and associated tag. For subscribing the attentive contents, the service provider is uploaded with the interests of the subscriber. For the storage of interests and uploaded tags, interest set and tag set is accomplished with the service provider and named as empty sets. When the subscription is arrived, in order to compete the interest and tag, the service provider sees to the tag. If there exists such a match, then the encrypted shared content related to this tag is sent by the service provider to the subscriber with that interest. Else, the interest is added to the interest set by the service provider and the subscriber is provided with False statement. When an uploaded tag is received by the service provider, it is handled in the same manner and this scheme is shown in the Figure 1.

Scheme 2: Content sharing with CP-ABE–PEKS: The main goal here is to guarantee the privacy of the shared content and the access policy is not allowed to leak. CP – ABE and PEKS are the building blocks that are used to concealing the subscriber identifications and access policy. The service provider estimates the licensed subscriber when encrypted credentials of subscriber is matched with encrypted access policy. The defining of access policy allows the publishers to specify who should access the shared content. For ensuring the confidentiality of the subscriber and publisher PEKS method is developed. The PEKS includes four algorithms such as KeyGen, PEKS, Trapdoor and Test. KeyGen can be executed by means of KGA where the attribute bi is taken as input and two keys namely public key ji and private key yi are taken as outputs. The leaves in the access tree are substituted with outputs of PEKS which encrypts the tag with public key ji of every attribute bi, hence access policies and tags are hidden. In order to hide the credentials of the subscriber, the encryption of interests or benefits with private key yi of every attribute bi, and the encryption process is handled by the trapdoor. Test matches with the trapdoor's output and PEKS output, when both the outputs match each other, Test will return True, else it will return False. CP-ABE-PEKS allows the service provider to determine the licensed subscribers without knowing about attributes, interests and tags. At every leaf node, the test is executed by matching algorithm. When encrypted tag matches with any interests that is encrypted then we can consider that leaf node is satisfied. The subscriber can

ISSN: 2582-1369 (online)
Submitted: 15.06.2021
Revised: 02.08.2021
Accepted: 18.08.2021
Published: 27.08.2021

Journal of ISMAC (2021)
Vol.03/ No.03
Pages: 250-262
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2021.3.006

be considered as the licensed one when the root also gets satisfied and so that the encrypted content can be forwarded.

Scheme 3: Publish–Subscribe System with Secure Proxy Decryption (PSSPD): The scheme 2 provides privacy to the shared content, the secrecy of subscriber and publisher is also preserved but only the licensed subscribers carries out the decryption of CP-ABE which may be challenging one in mobile environment. Scheme 3 solves all these disadvantages. The transformation key TK is also uploaded along with the credentials by the subscriber through which cipher text is transformed into EIGamal-style cipher text by the subscriber. The users calculate the exponentiation for recovering the shared content.

4. Results and Discussion

The result of the size of attribute set on generating ITK and Search key timing is shown by the Figure 2. When there is an increasing number in size of the attribute, there is a linear growth in generation time of search key and ITK. Because of the high computational complexity, the generation time of ITK is higher than the generation time of search key. From this we can conclude that the computational complexity can be represented as $\Theta(|A|)$, here the A is attribute set.

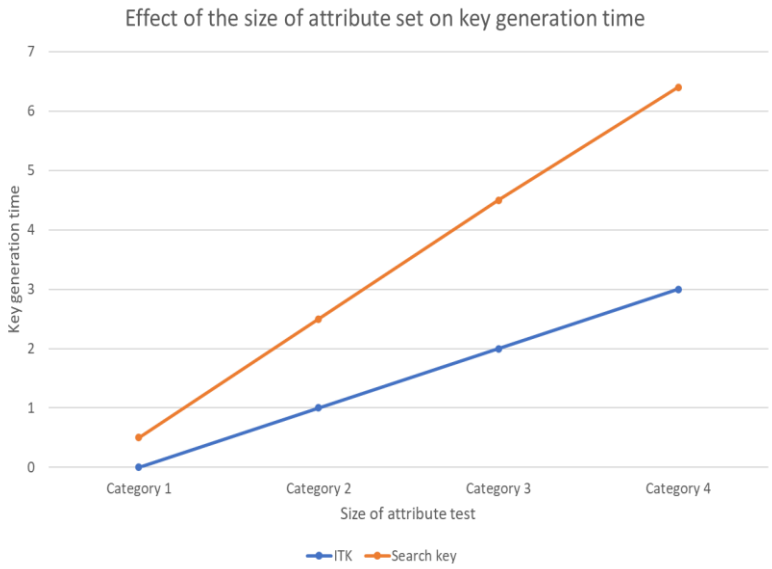

Figure 2. Effect of size of the attribute

ISSN: 2582-1369 (online)
Submitted: 15.06.2021
Revised: 02.08.2021
Accepted: 18.08.2021
Published: 27.08.2021

Journal of ISMAC (2021)
Vol.03/ No.03
Pages: 250-262
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2021.3.006

In Figure 3, there is a linear growth in encryption time of single subscriber when the size of the attribute set rises. When the interest set and size of the attribute set increases, the encryption time rises quadratically. Hence, the computational complication in encryption time of single subscriber is represented as $\Theta(|A'|.|I|)$, here I is interest set and A' is attribute set.

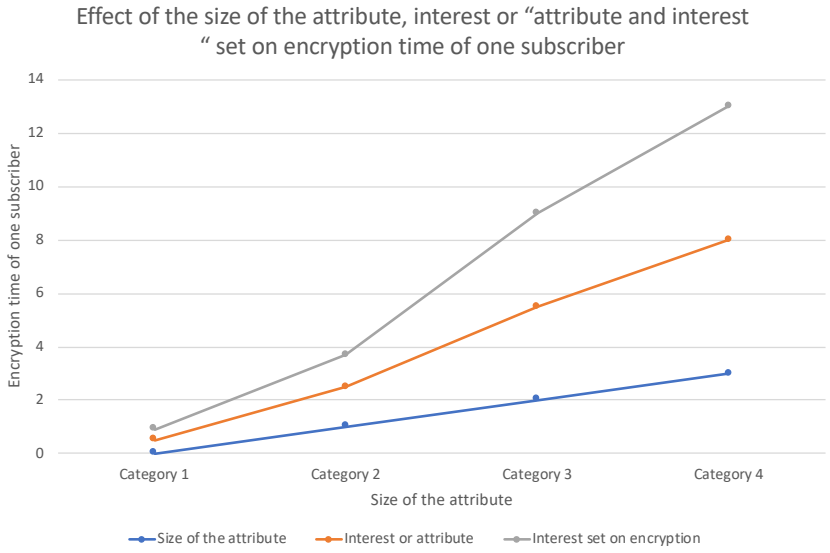

Figure 3. Effect of size of the attribute, interest or ''attribute and interest'' set on encryption time of one subscriber

5. Conclusion

A privacy preserving model of content sharing method with energy efficiency is proposed in this paper. This method does not leak any information to unlicensed parties and does not impose heavy burden to end users in terms of energy consumption. The user credentials and data confidentiality are protected by access control techniques that work on privacy preserving in a self-contained manner. Keyword search based public-key encryption with ciphertext policy attribute-based encryption is used efficiently. At the end users, ciphertext decryption reduces the energy consumption by the secure proxy decryption scheme. The routine of the privacy preserving content sharing scheme is improved by the proxy encryption and decryption process. In the future work, a more efficient method that still reduces the energy consumption will be proposed.

ISSN: 2582-1369 (online)
Submitted: 15.06.2021
Revised: 02.08.2021
Accepted: 18.08.2021
Published: 27.08.2021

Journal of ISMAC (2021)
Vol.03/ No.03
Pages: 250-262
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2021.3.006

References

[1] Miluzzo, E., Lane, N. D., Fodor, K., Peterson, R., Lu, H., Musolesi, M., ... & Campbell, A. T. (2008, November). Sensing meets mobile social networks: the design, implementation and evaluation of the cenceme application. In Proceedings of the 6th ACM conference on Embedded network sensor systems (pp. 337-350).

[2] Sivaganesan, D. "A Data Driven Trust Mechanism Based on Blockchain in IoT Sensor Networks for Detection and Mitigation of Attacks." Journal of trends in Computer Science and Smart technology (TCSST) 3, no. 01 (2021): 59-69.

[3] Hu, X., Chu, T. H., Leung, V. C., Ngai, E. C. H., Kruchten, P., & Chan, H. C. (2014). A survey on mobile social networks: Applications, platforms, system architectures, and future research directions. IEEE Communications Surveys & Tutorials, 17(3), 1557-1581.

[4] Moholkar, K. P., and S. H. Patil. "Deep Ensemble Approach for Question Answer System." In Computer Networks, Big Data and IoT, pp. 15-24. Springer, Singapore, 2021.

[5] Jin, L., Chen, Y., Wang, T., Hui, P., & Vasilakos, A. V. (2013). Understanding user behavior in online social networks: A survey. IEEE Communications Magazine, 51(9), 144-150.

[6] Manoharan, J. Samuel. "A Novel User Layer Cloud Security Model based on Chaotic Arnold Transformation using Fingerprint Biometric Traits." Journal of Innovative Image Processing (JIIP) 3, no. 01 (2021): 36-51.

[7] Suma, V., and Wang Haoxiang. "Optimal Key Handover Management for Enhancing Security in Mobile Network." Journal of trends in Computer Science and Smart technology (TCSST) 2, no. 04 (2020): 181-187.

[8] Agrawal, Prerna, and Bhushan Trivedi. "AndroHealthCheck: A Malware Detection System for Android Using Machine Learning." In Computer Networks, Big Data and IoT, pp. 35-41. Springer, Singapore, 2021.

[9] Huang, Q., Wang, L., & Yang, Y. (2017). Secure and privacy-preserving data sharing and collaboration in mobile healthcare social networks of smart cities. Security and Communication Networks, 2017.

ISSN: 2582-1369 (online)
Submitted: 15.06.2021
Revised: 02.08.2021
Accepted: 18.08.2021
Published: 27.08.2021

Journal of ISMAC (2021)
Vol.03/ No.03
Pages: 250-262
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2021.3.006

[10] Alam, M. F., Katsikas, S., Beltramello, O., & Hadjiefthymiades, S. (2017). Augmented and virtual reality based monitoring and safety system: A prototype IoT platform. Journal of Network and Computer Applications, 89, 109-119.

[11] Adithya, M., P. G. Scholar, and B. Shanthini. "Security Analysis and Preserving Block-Level Data DE-duplication in Cloud Storage Services." Journal of trends in Computer Science and Smart technology (TCSST) 2, no. 02 (2020): 120-126.

[12] Xiao, X., Chen, C., Sangaiah, A. K., Hu, G., Ye, R., & Jiang, Y. (2018). CenLocShare: A centralized privacy-preserving location-sharing system for mobile online social networks. Future Generation Computer Systems, 86, 863-872.

[13] Ismagilova, E., Hughes, L., Rana, N. P., & Dwivedi, Y. K. (2020). Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework. Information Systems Frontiers, 1-22.

[14] Dhanya, V. G., Minu Susan Jacob, and R. Dhanalakshmi. "Twitter-Based Disaster Management System Using Data Mining." In Computer Networks, Big Data and IoT, pp. 193-203. Springer, Singapore, 2021.

[15] Sahoo, S. R., & Gupta, B. B. (2019). Classification of various attacks and their defence mechanism in online social networks: a survey. Enterprise Information Systems, 13(6), 832-864.

[16] Joe, Mr C. Vijesh, and Jennifer S. Raj. "Location-based Orientation Context Dependent Recommender System for Users." *Journal of trends in Computer Science and Smart technology (TCSST)* 3, no. 01 (2021): 14-23.

[17] Zhang, G., Li, T., Li, Y., Hui, P., & Jin, D. (2018). Blockchain-based data sharing system for ai-powered network operations. Journal of Communications and Information Networks, 3(3), 1-8.

[18] AlOsail, Deemah, Noora Amino, and Nazeeruddin Mohammad. "Security Issues and Solutions in E-Health and Telemedicine." In Computer Networks, Big Data and IoT, pp. 305-318. Springer, Singapore, 2021.

[19] Chitra, Ms K., and V. PRASANNA Venkatesan. "An antiquity to the contemporary of secret sharing scheme." Journal of Innovative Image Processing (JIIP) 2, no. 01 (2020): 1-13.

[20] Ranganathan, G. "Real time anomaly detection techniques using pyspark frame work." Journal of Artificial Intelligence 2, no. 01 (2020): 20-30.

ISSN: 2582-1369 (online)
Submitted: 15.06.2021
Revised: 02.08.2021
Accepted: 18.08.2021
Published: 27.08.2021

Journal of ISMAC (2021)
Vol.03/ No.03
Pages: 250-262
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2021.3.006

[21] Du, J., Jiang, C., Han, Z., Zhang, H., Mumtaz, S., & Ren, Y. (2017). Contract mechanism and performance analysis for data transaction in mobile social networks. IEEE Transactions on Network Science and Engineering, 6(2), 103-115.

[22] Kanade, Vijay A. "A Novel IoT Device for Optimizing “Content Personalization Strategy”." In Computer Networks, Big Data and IoT, pp. 627-634. Springer, Singapore, 2021.

[23] Valanarasu, Mr R. "Comparative Analysis for Personality Prediction by Digital Footprints in Social Media." *Journal of Information Technology* 3, no. 02 (2021): 77-91.

[24] Pandian, A. Pasumpon. "Performance Evaluation and Comparison using Deep Learning Techniques in Sentiment Analysis." *Journal of Soft Computing Paradigm (JSCP)* 3, no. 02 (2021): 123-134.

[25] Devi, S. Sathiya, and R. Rajakumar. "Network Intrusion Detection Using Cross-Bagging-Based Stacking Model." In Computer Networks, Big Data and IoT, pp. 743-751. Springer, Singapore, 2021.

[26] Guidi, B., Conti, M., Passarella, A., & Ricci, L. (2018). Managing social contents in decentralized online social networks: A survey. Online Social Networks and Media, 7, 12-29.

[27] Suma, V. "Community Based Network Reconstruction for an Evolutionary Algorithm Framework." *Journal of Artificial Intelligence* 3, no. 01 (2021): 53-61.

[28] Rath, M. (2018, April). An analytical study of security and challenging issues in social networking as an emerging connected technology. In Proceedings of 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT) (pp. 26-27).

[29] Okello Candiya Bongomin, G., Ntayi, J. M., Munene, J. C., & Malinga, C. A. (2018). Mobile money and financial inclusion in sub-Saharan Africa: the moderating role of social networks. Journal of African Business, 19(3), 361-384.

[30] Qiu, T., Chen, B., Sangaiah, A. K., Ma, J., & Huang, R. (2017). A survey of mobile social networks: Applications, social characteristics, and challenges. IEEE systems journal, 12(4), 3932-3947.

[31] Li, W., Luo, S., Sun, Z., Xia, Y., Lu, L., Chen, H., ... & Guan, H. (2018, June). Vbutton: Practical attestation of user-driven operations in mobile apps. In Proceedings of the 16th annual international conference on mobile systems, applications, and services (pp. 28-40).

ISSN: 2582-1369 (online)
Submitted: 15.06.2021
Revised: 02.08.2021
Accepted: 18.08.2021
Published: 27.08.2021

Journal of ISMAC (2021)
Vol.03/ No.03
Pages: 250-262
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2021.3.006

[32] Al-Qurishi, M., Rahman, S. M. M., Hossain, M. S., Almogren, A., Alrubaian, M., Alamri, A., ... & Gupta, B. B. (2018). An efficient key agreement protocol for Sybil-precaution in online social networks. Future Generation Computer Systems, 84, 139-148.

[33] Wang, X., Ning, Z., Zhou, M., Hu, X., Wang, L., Zhang, Y., ... & Hu, B. (2018). Privacy-preserving content dissemination for vehicular social networks: Challenges and solutions. IEEE Communications Surveys & Tutorials, 21(2), 1314-1345.

Author's biography

Jennifer S. Raj received the Ph.D degree from Anna University and Master's Degree in communication System from SRM University, India. Currently she is working in the Department of ECE, Gnanamani College of Technology, Namakkal, India. She is a life member of ISTE, India. She has been serving as Organizing Chair and Program Chair of several International conferences, and in the Program Committees of several International conferences. She is book reviewer for Tata Mc Graw hill publication and publishes more than fifty research articles in the journals and IEEE conferences. Her interests are in wireless Health care informatics and body area sensor networks.

ISSN: 2582-1369 (online)
Submitted: 15.06.2021
Revised: 02.08.2021
Accepted: 18.08.2021
Published: 27.08.2021