Journal of Excellence in Computer Science and Engineering, Vol. 1(2) 2015, pp. 1-10

RESEARCH ARTICLE

Secured Friending in Proximity based Mobile Social Network

***Y Vidya[1], B Shemimol [2]**

[1]PG Scholar, Department of Computer and Information Science, TKM Institute of Technology, Kollam, Kerala, India.

[2]Assistant Professor, Department of Computer Science, TKM Institute of Technology, Kollam, Kerala, India.

Received-18 November 2015, Revised-14 December 2015, Accepted-15 December 2015, Published-28 December 2015

ABSTRACT

In recent days there is a tremendous rise in the need of proximity based mobile social networks. The basic function is to find friends in close proximity with matching profiles securely which is crucial. The earlier profile matching models directly publish the user profiles while searching friends with matching profiles. User profiles may contain many confidential details which the users are unwilling to share with strangers. In this paper we use privacy preserving protocols with two levels of privacy along with advanced encryption standard to securely find friends with matching profiles in close proximity which is the primary goal. We do not use any trusted central server. Hence our system is distributed. In this paper we also provide security for the shared data associated with multiple users with the help of a multi-party access control model which is the secondary goal of our system. Evaluation using real data and actual implementation shows that this mechanism improves security and is privacy preserving, verifiable and efficient.

Keywords: Friending, Profiling, Proximity, Profile matching, Multi party access control model, Privacy.

1. INTRODUCTION

The conflux of social network, smart phone devices and location based services, has driven significant changes across the mobile computing prospect. Mobile users and developers are verifying new means to collaborate with their physical environment using web and mobile phones. Ingenious mobile application vendors bring applications to the market that allow mobile users connect and interact with people in close proximity. They expect this raising market-Proximity based Mobile Social Network(PMSN) to grow to $ 1.9 billion in revenue by 2016. This trend not only provides fortuity for application providers but also has potential to agitate the current social networking market. Proximity based mobile social network refers to the interaction among people in the nearby proximity within a WIFI or bluetooth connection. Friending and communication are the two basic functions of MSNs. People join the social network by creating their own user profile and then interact with other users. Profile matching means two users compare their personal profiles and is a common and useful way to make new friends with common interests.

The ideal situation is to let the initiator and its best matching user directly and privately find out and interact with each other without knowing anything about other users profile attributes. This is a challenging situation. Some applications help a user to find other users with similar profile within a certain distance automatically. MagnetU matches one

*Corresponding author. Tel.: +919895102130
Email address: vidya.y8@gmail.com (Y.Vidya)
Double blind peer review under responsibility of DJ Publications
http://dx.doi.org/10.18831/djcse.in/2015021001

with nearby users for friend making based on common interest. E- Small talker [1] matches people interest before initiating a talk. These applications uses user profile for friending between nearby strangers and enable privacy preserving among people to some extent.

Friending means finding and approaching the right friends. People are unwilling to disclose their personal profiles to strangers within physical proximity before deciding to connect with them. The insecure wireless communication channel and potentially untrusted service provider increase the risk of revealing private information. Many approaches [1, 2, 3, 4] were introduced in order to solve the problem of privacy preserving profile matching. In the existing system [4] proposed two privacy preserving profile matching schemes, the PSI(Private Set Intersection) and PCSI(Private Cardinality Set Intersection) schemes .They also leveraged Secure Multiparty Computation (SMC) and Shamir Secret share schemes(SS) for efficient computation and communication. It introduced two increasing levels of privacy with decreasing amount of revealed profile information. This relays on homomorphic encryption which is non-verifiable. In our system communication is done between strangers. Since the strangers do not exchange their keys, using different keys is not verifiable.

An MSN provides each user with a virtual space containing profile information. A user profile includes information regarding user's birthday, gender, interest, education and work history etc. A user can not only upload content into their own space but also include other users by tagging them. Tagging explicitly links tagged users profile. The privacy of these contents is a crucial one. The existing system does not provide security for shared data. Primarily MSNs provide simple methods to protect the content on own space, but do not provide any security measures for those shared on others space. In this paper we overcome these challenges and introduce the following contributions:

1. We propose an effective and tractable control mechanism for MSN, accommodating the spatial authorization requirements coming from allied users for managing the shared data. Some typical data sharing patterns with respect to multiparty authorization in MSN are also identified. Based on these sharing patterns an MPAC (Multi Party Access Control) [9] model is framed to capture the core features of multiparty authorization requirements that have not been given so far by existing access control systems and models for MSNs.
2. We introduce AES algorithm in order to improve verifiability and protection.

2. RELATED WORK

In sync with our works a secure friendly discovery protocol is introduced in [2]. Different from us, the similarity is computed using dot product mechanism and not by finding intersection as in our work. It also requires a centralized trusted authority for its control. In [3] a private contact discovery protocol is introduced where the access to private contact is controlled using distributed certification. In general, a distributive certificate is not suitable for rest of the sensitive data. It is restricted to certain profile attributes. Our work is not limited to the type of profile attributes. In [16, 17] privacy preserving multiparty interest sharing protocols for smart phone is proposed. It utilizes an online semi trusted server which is not available when there is no connection. Several access control models have been introduced in [10, 11, 12, 13, 14, 15] to control shared data. In [8] they proposed a semi-decentralized access control model and a related mechanism for controlled sharing of information. [9] describes a relationship based access control (ReBAC) as security paradigm. It formulated the ReBAC model that provides authorization decision based on the relationship between resource owner and resource accessor in MSN. [14] recommended the access control mechanism framed in facebook admitting arbitrary policy vocabularies that are based on graph properties. None of this existing works provide collaborative management of shared data in MSN.

In this paper we propose two fully distributed privacy preserving profile matching schemes that provide two user selective levels of privacy. Our system is decentralized and there is no trusted third party. We exploit the verifiability of AES encryption. We propose a novel method for collaborative management of shared data associated with multiparty along with certain access policies and policy evaluation mechanisms, thus improving the data security.

3. PROBLEM DEFINITION

3.1. System model

Our system consists of a set of users each owning a mobile device in which a PMSN application is installed. We assume that the devices are securely connected via Wi-Fi. We assume every user is in the communication range of each other. On connecting to the network each participant creates his own user profile. A profile acts as the unique fingerprint of the user in a mobile social network. The protocols are run by each user with every other user profiles within the proximity and find the one with matching profiles which is the primary goal of our system. We do not assume any trusted central authority during protocol run and hence profile matching is done in a completely distributed way. Data is shared among a set of users and is revealed only if there exist the share of a minimum number of users, thus protecting the sensitive data from hackers. Our system with the help of a multi-party access control model controls the data shared among matching users. Each user makes different decisions on a single shared data, the access control model with the help of different access control policies i.e.; to whom they are to be made visible. The block diagram for our system is given in figure B1and figure B2.

Figure B1 explains the profile matching architecture. Here a user logs in to his home page with his user id and password. A new user registers with his details in order to get connected. In his home page he is listed with all the proximate users. Each user can select their privacy levels manually. Two privacy levels are set up viz PL1 and PL2. PL1 is achieved using basic scheme and PL2 using advanced scheme. User set up his privacy level while registering with a PMSN. Basic scheme and advanced scheme initially contains three steps: data share distribution, computation and reconstruction. In advanced scheme an additional scheme blind and permute is involved. The input here is the set of attributes users have. Basic scheme and advanced scheme gives the attribute of intersection and cardinality of intersection as output respectively. Blind and permute is used to compute the cardinality of intersection. Selecting a participant from the listed proximate users open up his profile, where one can see the intersecting attributes or the percentage of intersection (based on the privacy scheme selected) with them. Thus the participants can select the one with highest matching and send request for further communication. AES algorithm is used for further encryption of profile attributes. Users can post and share resources on their own space or of the others. A single resource can be accessed by multiple users at the same time. The shared data can be managed using MPAC model. Figure B2 explains the MPAC architecture. When multiple users access a shared data, multiparty access control policies are set up in order to collaboratively manage them. The policy is evaluated to obtain a decision for each party. The decisions obtained are aggregated to form a final decision i.e. to access or deny permission to the shared data.

3. PRIVACY PRESERVING AND SECURED FRIENDING

4.1. Privacy preserving

4.1.1. Overview

In this paper we adopted two profile matching schemes, a basic and an advanced one proposed by [4, 5, 6, 7] with one privacy level each. We use the basic schemes PSI for Privacy Level 1 (PL1) and the advanced scheme PCSI for Privacy Level 2 (PL2).

Two sets of user computation set and reconstruction set are defined below: Definition 1(Computation set): A set of parties $Þi$ who help P1 and Pi to compute the share of $F_i(x_j)$, $1 \leq j \leq n$, which include P1 and Pi.
Definition 2(Reconstruction set): A set of parties $Þi' \subset P$ who will compute the shares of $F_i(x_j), 1 \leq j \leq n$ for reconstruction, which include P1 and Pi (Table A1)

4.1.2. Basic scheme

The basic scheme is based on the secure polynomial evaluation using secret sharing. Here the initiator (P_1) and other candidates Pi, share their inputs among the computation set, $Þi$ (subset of Pi) using Shamir Secret share (SS). Þi then jointly computes the shares of function $F_i(x_j) = R_{ij} \cdot f_i\ (x_j) + x_j$ for each $1 \leq j \leq n$, where $f_i(y)$ is the polynomial representing P_i's set and R_{ij} is the random number jointly generated by P_1 and P_i and not known to anyone.

$xj \in I_{1j}$ iff $F_i(x_j) = x_j$.The value of $F_i(x_j)$ remain in secret shared form between them before the shared are revealed. The whole is done in three steps: data share distribution, computation and reconstruction. In order to reduce the computation complexity the scheme was proposed, that combines multiple multiplication and addition into one round during secure polynomial evaluation.

4.1.3. Advanced scheme

In the advanced scheme the parties in Þi first compute the shares of function $F_i(x_j) = R_{ij}.f_i(x_j), 1 \leq j \leq n$ securely using basic scheme where $x_j \in I_{1i}$iff. $R_{ij}F_i(x_j) = 0$. In order to hide from P1 the relation between its input x_j ,$1 \leq j \leq n$ and ouput $F_i(x_j)$ a blind and permute method [4] is used.
The basic scheme and advanced scheme are detailed in [4]

4.2. Secured friending

4.2.1. Multi Party Access Control model

In this paper, we pursue a systematic solution to facilitate collaborative management of shared data in MSN with the help of MPAC model, a policy scheme and a policy evaluation mechanism. MSN provide a user with a web space where the user can store and manage personal data. Several access control schemes [12, 13, 14] were introduced to protect these personal data but they allow only single controller i.e. the content owner to specify access control policy. This paper introduces a mechanism proposed by [9] that supports multiple controllers such as owner (one who owns data), distributor (one who shares data to someone else's space), tagged users and sharer (one who shares data from someone else's space), who are associated with shared data to specify access control policy.

4.2.2. MPAC policy specification

In order to collaboratively manage the shared data multiparty access control policies are set up on them, which specifies the authorization requirements from multiple associated users. Multiparty access control policy is a five tuple: P=< controller; type; authoriser; data; result>, where

- Controller ∈ U is a user who can regulate the access of data.
- Type ∈ CT is the type of controller.
- Authoriser is a set of users to whom the authorisation is granted, representing with an access specification.
- Data is represented with a data specification.
- Effect ∈ {permit; deny} is the authorisation effect of the policy.

4.2.3. MPAC policy evaluation

Two steps are performed to evaluate the access control policies. First one is to check the access request against the policy specified by each controller and yields a decision for the controller. Accessor element checks whether that policy is applicable to a request. If the user who sends the request belong to the set of users derived from the accessor policy then the policy is applicable and evaluation process returns with a result (permit/deny). In the final step decisions on the access request from all controllers are aggregated to form the final decision for the access request. Figure B2 illustrates the policy evaluation mechanism.

Since data controllers produce different access request for a single content, there may arise conflicts. In order to make precise access decision certain conflict resolution mechanism is necessary during multiparty policy evaluation. The simplest solution is to allow only the common users in accessor set derived by multiple controllers to access the data. But this is very restrictive and may not provide effective conflict resolution. Hence certain conflict resolution mechanisms were derived in [9].

5. RESULT AND DISCUSSION

The system analysis shows that our system is secure, privacy preserved, verifiable and efficient based on our assumptions.

5.1. Security analysis

The existing basic and advanced schemes provide the basic security to the system. Replacing the additive homomorphic encryption used in the existing system with AES improved security to user profile. The multiparty access control model introduced here increases the security to the shared data associated with multiple users. Thus the proposed system is more secure compared to existing system. Figure B3 is the security graph. Here x-axis represents percentage

security, y-axis represents the system. It shows the security hike of the proposed system, with the addition of MPAC and AES with respect to the existing system which uses homomorphic encryption.

5.2. Verifiability

In this system communication is done between strangers. The additive homomorphic encryption used in the existing system is non-verifiable. Using different keys for encryption and decryption do not provide any provision for any two users to verify the correctness of what is done at the two ends since the users are strangers and they may not be willing to exchange their secret keys. Use of AES encryption in the proposed system increases verifiability.

5.3. Efficiency

Performance of a system is evaluated based on computation and communication cost. Addition of AES encryption in the proposed system cuts down the computation cost to a fraction. AES is efficient than any other encryption standard. Addition of MPAC for collaborative management of shared data improves the efficiency of the system. Figure B4 is the execution time graph. In this graph, x- axis represents the encryption algorithm used in the existing system using additive homomorphic encryption and proposed system using AES encryption. Y-axis represents the execution time (ms). It explains the decrease in execution time by replacing the additive homomorphic encryption in the existing system with AES encryption in the proposed system.

6. CONCLUSION

In this paper we adopt two specific protocol schemes PSI (Private Set Intersection) and PCSI (Private Cardinality Set Intersection) for privacy preserved profile matching which was used in the existing system, by replacing the additive homomorphic encryption, which is non-verifiable with AES algorithm. Leveraging AES makes it more secure and verifiable so that the attacker attacks only the encrypted data. The existing system does not provide any security for shared data associated with multiple users. This paper introduces a novel solution for collective management of shared data associated with multiple users in proximity based mobile social network called MPAC (Multi Party Access Control) model. Based on our assumptions the proposed system increases system security, and is verifiable, privacy preserving and efficient than the existing one. The system can be verified with other profile matching schemes with high performance and can be considered as our future work.

REFERENCES

[1] Z.Yang, B.Zhang, J.Dai, A.Champion, D.Xuan and D.Li, Esmalltalker: A Distributed Mobile System for Social Networking in Physical Proximity,2010 International Conference on Distributed Computing Systems, Genova, Italy, 2010, pp. 1535 – 1545.

[2] W.Dong, V.Dave, L.Qiu and Y.Zhang, Secure Friend Discovery in Mobile Social Networks, Proceedings IEEE INFOCOM, China, 2011, pp. 1–9.

[3] De Cristofaro, M.Manulis, and B.Poettering, Private Discovery of Common Social Contacts, Applied Cryptography and Network Security, Proceedings 9th International Conference, ACNS, Nerja, Spain, 2011, pp. 147–165.

[4] Ming Li, Shucheng Yu, Ning Cao and Wenjing Lou, Privacy-Preserving Distributed Profile Matching in Proximity-based Mobile Social Networks IEEE transactions on wireless communications, Vol. 12, No. 5, 2013, pp. 2024 – 2033.

[5] M.Li, N.Cao, S.Yu and W.Lou, FindU: Privacy-Preserving Personal Profile Matching in Mobile Social Networks, Proceedings IEEE INFOCOM, Shanghai, China, 2011, pp. 1–9.

[6] A.Shamir, How to share a secret, Communications of the ACM, vol. 22, no. 11, 1979, pp. 612–613, http://dx.doi.org/10.1145/359168.359176.

[7] R.Gennaro, M.O.Rabin and T.Rabin, Simplified VSS and Fast-Track Multiparty Computations with Applications to Threshold Cryptography, Proceedings of the Seventeenth Annual ACM Symposium on Principles of Distributed Computing, pp. 101-111, http://dx.doi.org/10.1145/277697.2777

16.

[8] R.Cramer, I.Damgard and J.Nielsen, Secure Multiparty Computation, Book draft, 2010.

[9] Hongxin Hu, S.Gail-Joon Ahn and Jan Jorgensen, Multiparty Access Control for Online Social Networks: Model and Mechanisms, IEEE Transactions on Knowledge and Data Engineering, Vol. 25, No. 7, 2013, pp. 1614-1627.

[10] D.Cristofaro and G.Tsudik, Practical Private Set Intersection Protocols With Linear Complexity, Financial Cryptography and Data Security, 14th International Conference, FC, Tenerife, Canary Islands, 2010, pp 143-159, http://dx.doi.org/10.1007/978-3-642-14577-3_13.

[11] M.Freedman, K.Nissim and B.Pinkas, Efficient Private Matching and Set Intersection, Advances in Cryptology – EUROCRYPT, International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, 2004, pp. 1–19, http://dx.doi.org/10.1007/978-3-540-24676-3_1.

[12] B.Carminati, E.Ferrari and A.Perego, Rule-Based Access Control for Social Networks, Proceedings of the International Conference on the Move to Meaningful Internet Systems, France, 2006, Pages 1734-1744, http://dx.doi.org/10.1007/11915034_99.

[13] B.Carminati, E.Ferrari and A.Perego, Enforcing Access Control in Web-Based Social Networks, ACM Transactions Information and System Security, vol. 13, no. 1, 2009, pp. 1-38, http://dx.doi.org/10.1145/1609956.1609962.

[14] P.Fong, Relationship-Based Access Control: Protection Model and Policy Language, Proceedings of the first ACM Conference on Data and Application Security and Privacy, San Antonio, Texas, 2011, pp. 191-202, http://dx.doi.org/10.1145/1943513.1943539.

[15] P.Fong, M.Anwar and Z.Zhao, A Privacy Preservation Model for Face book-Style Social Network Systems, Proceedings of the 14th European conference on Research in Computer Security, pp. 303-320, 2009.

[16] De Cristofaro, A.Durussel and I.Aad, Reclaiming Privacy for Smart Phone Applications, IEEE International Conference on Pervasive Computing and Communications, Seattle, USA 2011, pp.84-92.

[17] R. Lu, X. Lin, X. Liang, and X. Shen, A secure handshake scheme with symptoms matching for mhealthcare social network, Mobile Networks and Applications, pp. 1–12, 2010, http://dx.doi.org/10.1007/s11036-010-0274-2

APPENDIX A

Table A1.Main notation

$\boldsymbol{N}, \boldsymbol{t}$	Number of parties, maximum number of colluders
$[\boldsymbol{s}]_{\boldsymbol{i}}^{\boldsymbol{t},\boldsymbol{w}}$	Party $\boldsymbol{Pi}$'s secret share of $\boldsymbol{s}$ (under $(\boldsymbol{t}, \boldsymbol{w})$ −SS)
$\boldsymbol{S_1}, \boldsymbol{S_i}$	$\boldsymbol{P1}$'s query attribute set, and $\boldsymbol{Pi}$'s profile attribute set
$\boldsymbol{x_j}, \boldsymbol{1 \leq j \leq n}$	$\boldsymbol{P1}$'s query set elements, $\boldsymbol{n} = [\boldsymbol{S1}\}$
$\boldsymbol{y_{ij}}, \boldsymbol{1 \leq j \leq m}$	$\boldsymbol{Pi}$'s profile set elements, $\boldsymbol{m} = [\boldsymbol{Si}], \boldsymbol{iE}\{\boldsymbol{2}, \ldots \boldsymbol{N}\}$
$\boldsymbol{I_{1,i}}$	Intersection set between $\boldsymbol{P1}$ and $\boldsymbol{Pi}$;$\boldsymbol{m1}, \boldsymbol{i} = \lvert \boldsymbol{I1}, \boldsymbol{i} \rvert$
$\mathrm{F}_{\boldsymbol{p}}$	The finite field used ;$\boldsymbol{k} = \boldsymbol{logp}$; security parameter
$\boldsymbol{H}(\,)$	A cryptographic hash function
$\overset{\boldsymbol{R}}{\leftarrow}, \lvert\lvert$	Random sampling from a set, concatenation
$\boldsymbol{P}, \boldsymbol{P_1}, \boldsymbol{P_i}$	The set of all parties, the initiator and the ith party
$\text{Þ}, \text{Þ}_{\boldsymbol{i}}'$	The computing set and reconstruction set for $\boldsymbol{Pi}$

APPENDIX B

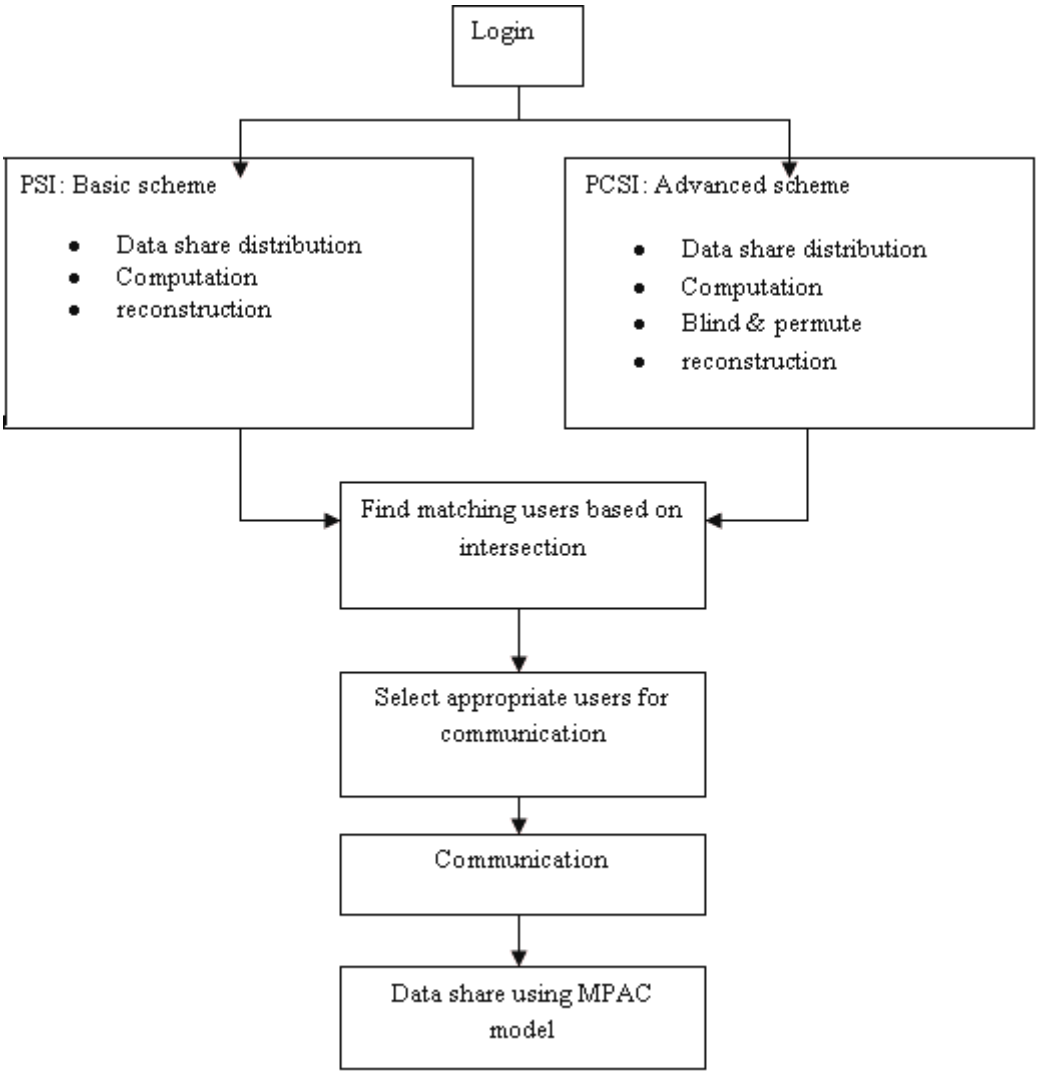

Figure B1.System architecture

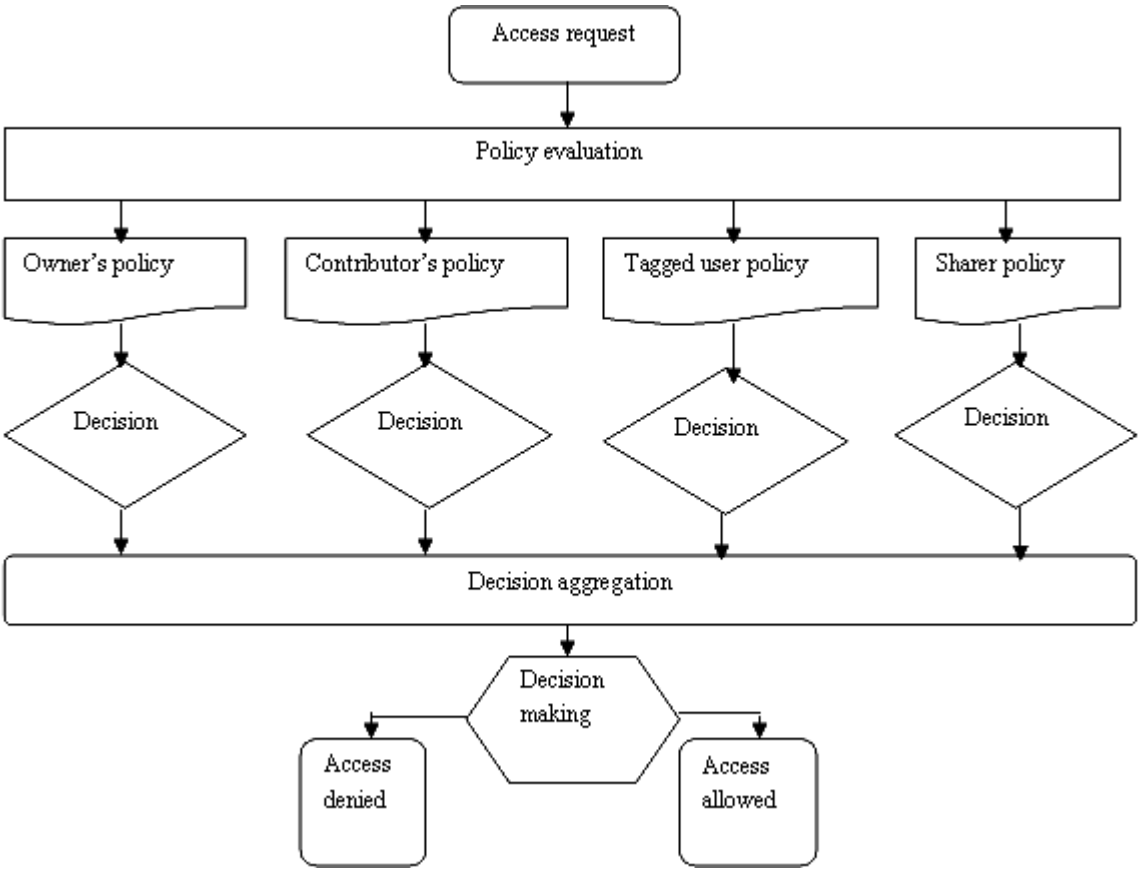

Figure B2. MPACK block diagram

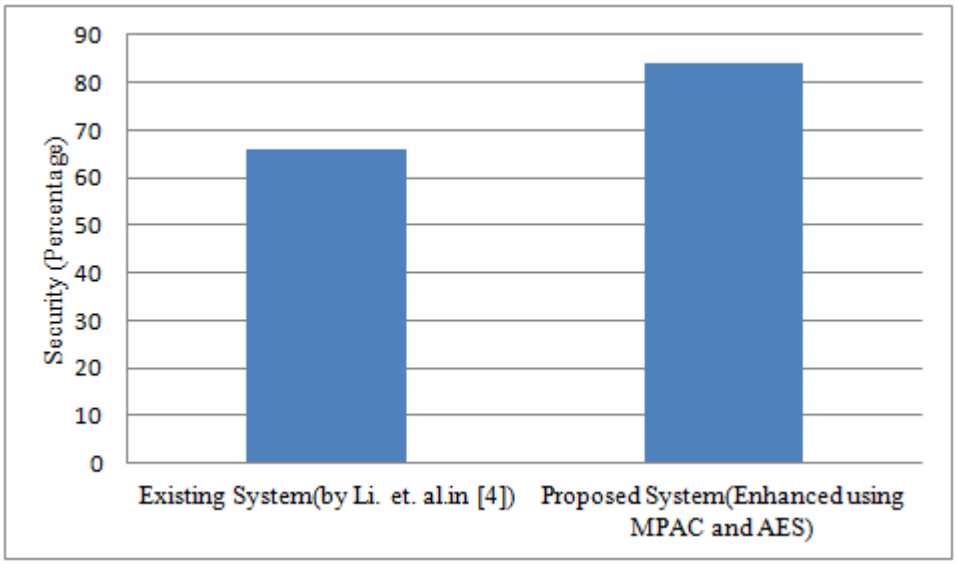

Figure B3.Security graph: Plotted against security and the system.

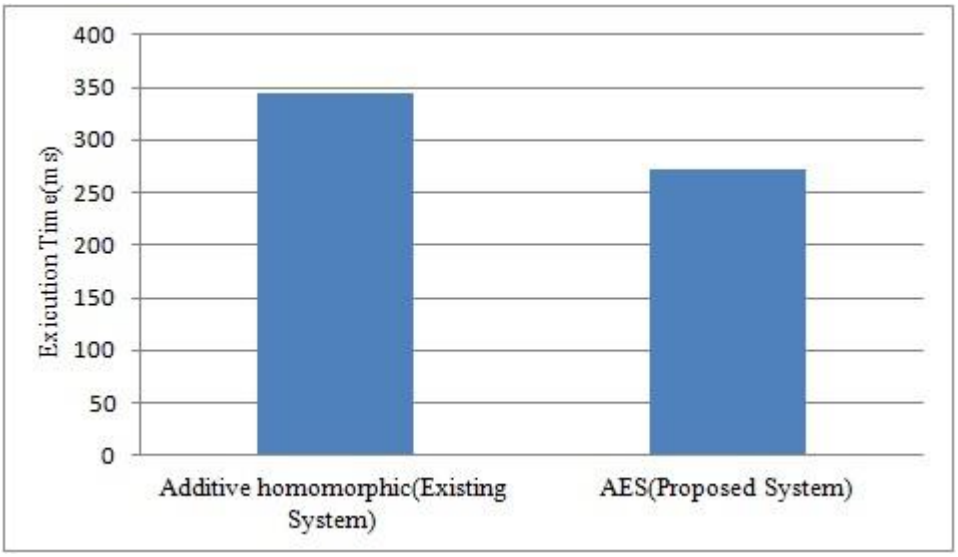

Figure B4.Execution Time Graph: Plotted against encryption algorithm and execution time.