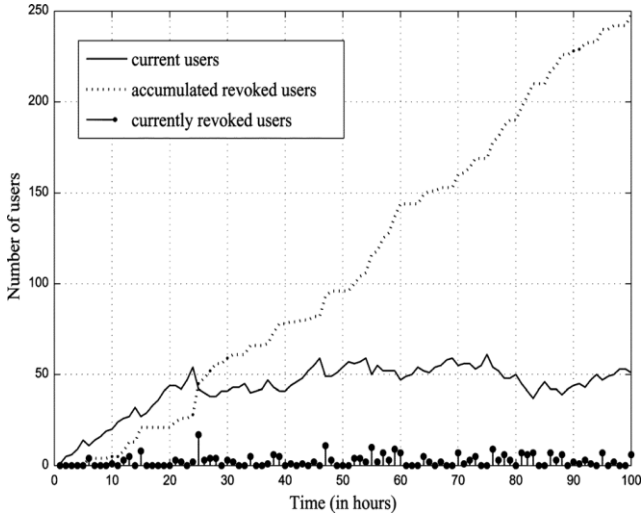

Figure 1: Number of users in an attribute group

4. Proposed System

An attribute-based secure data retrieval scheme using CP-ABE for decentralized DTNs [2][5]. They are three types: First, immediate attribute revocation will help the backward/forward data will be squired. Second, encryptors will find a fine-grained access policy authorities [2][3].Third, the key escrow problem is resolved by an escrow-free key using DTN architecture. [5][6][7].

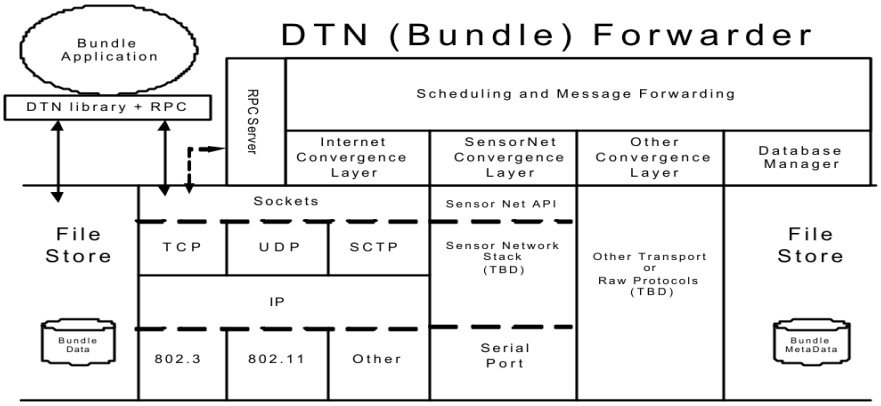

FIGURE 2. Structure of a DTN forwarder. Multiple *convergence layers*, one per protocol stack, provide a common interface to the message scheduler/forwarder.

The key problem faced by the protocol generates and issues user the secret keys by performing secure two-party computation protocol among the key authorities with their own master key[9][7].The 2PC protocol try the key authorities to obtain any master key information of each other so that none of them will generates the key. ADVANTAGES OF PROPOSED SYSTEM: **Data confidentiality, Collusion-resistance & Backward and forward Secrecy**

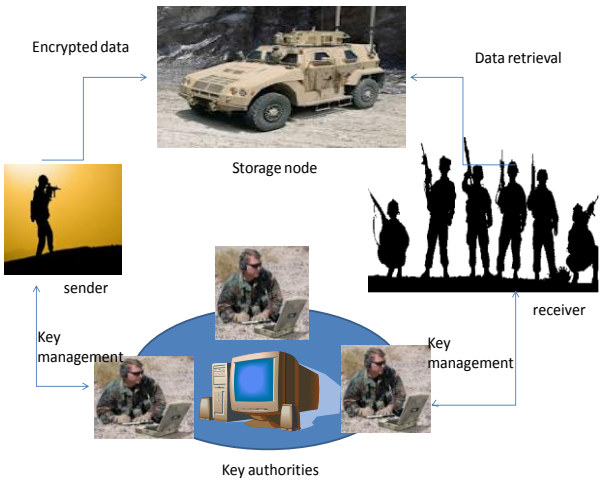

Figure 3: Architecture of secure data retrieval in a DTNs network.

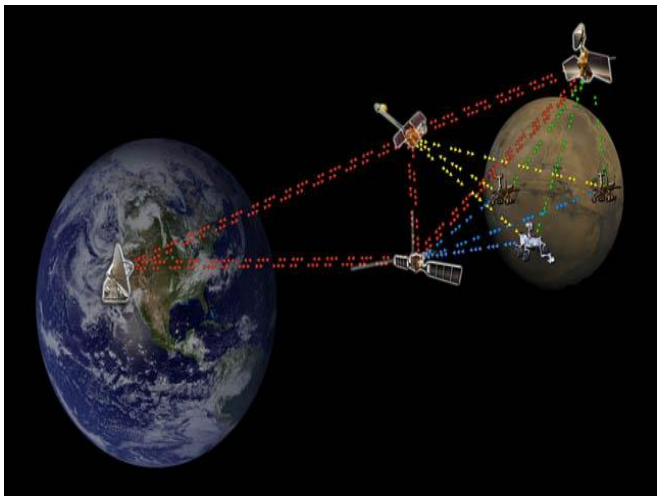

Figure 4: DTN used for Mars rover communication

5. Implementation

Analysis is the process of finding the best solution to the problem. System analysis is processed by learn about the existing problems, define objects and requirements and evaluates the solutions [7][9]. It is the way of thinking about the organization and the problem it involves, a set of technologies that helps in solving these problems.

Identification and design of the modules for implementing [8][10].

Feasibility Report: Depending on the results of the expanded to a more detailed feasibility study. By testing the system proposal according to its works, impact of the organization, ability to meet needs and effective use of the resources [6][7]. This determines the evaluate performance and cost effective of each proposed system. Select the best proposed system. Three key considerations involved in the feasibility analysis are:

- Economical Feasibility
- Technical Feasibility
- Social Feasibility

6. Conclusion

DTN technologies are successful solutions in army network applications that allow wireless devices to transmit the information is kept securely and then sends the information to all external storage nodes.

CP-ABE is a scalable cryptographic solution to the access control and secures data retrieval issues. The inherent key escrow problem is resolved such that the confidentiality of the stored data is guaranteed even under the hostile environment where key authorities might be compromise or not fully trusted. We demonstrate how to apply the proposed mechanic securely and efficiently manage the confidential data distributed in the disruption tolerant army network.

References

[1] R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable secure file sharing on storage," 2006
[2] J. Burgess, B. Gallagher, D. Jensen, and B. N. Levine, " Routing for vehicle-based disruption networks," 1–11.2006
[3] M. Chuah and P. Yang, "Node density-based adaptive for disruption tolerant networks,"
[4] M. M. B. Tariq, "Mesage ferry route design for sparse ad hoc networks with mobile nodes," 2006
[5] M. Chuah and P. Yang, "Performance based on information retrieval schemes for DTNs," pp. 1–7.2007
[6] M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Mediated CP-ABE and its application".2007
[7] M. Chuah, "Secure data retrieval based on (CP-ABE) system for the DTNs," Lehigh CSE Tech. Rep., 2009.
[8] A. Sahai, and B. Waters, "ABE with non-monotonic access structures," 2010
[9] J. Bethencourt, A. Sahai, and B. Waters, "Cipher text-policy encryption," 2010
[10] V.Goyal, A. Jain,O. Pandey, andA. Sahai, "Bounded CP-ABE," in *Proc. ICALP*, 2010, pp. 579–591.