INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN 2278 – 0211 (Online)

Application of Data Self-Destructing System Online

Pravin M. Sonsare
Assistant Professor, Shri Ramdeobaba College of Engineering and Management, Nagpur, India
Khushbu R. Khandait
Assistant Professor, Govindrao Wanjari College of Engineering and Technology, Nagpur, India

Abstract:
Fast growing Internet leads to the question of security of information uploaded or stored online. Personal data stored in the Cloud may contain account numbers, passwords, notes, and other important information that could be used and misused by a miscreant, a competitor, or a court of law. These data are cached, copied, and archived by Cloud Service Providers (CSP's), often without users authorization and control. Aim of self-destructing data is to protect private personal data. All the data and their copies become scribbled after a user-specified time, without any user intervention. In this system we are using a shamir's secret share algorithm for making the system more effective for the privacy purpose. The shamir algorithm splits the session key generated and passes that key to server and the client. In this system any type of information transfer is not done. So the user's data privacy is maintained. Active storage framework is used to store this data so the system is called SEDAS (self destructing data storage using active storage framework).
Through functionality and security properties evaluations of the SeDas prototype, the results demonstrate that SeDas is practical to use and meets all the privacy- preserving goals described. Compared to the system with self-destructing data mechanism.

Keywords: *privacy, CSP (Cloud Service Providers), prototype, SeDas*

1. Introduction

The proposed system that is application of self destructing data system for cloud environment. In this system data get automatically destructed after the user specified time given to the system without the user intervention. The all user copies become unreadable for the outside user of the system. It protects the user's data privacy. The cloud contain or it fetches the users confidential data so that compromises the privacy and the security of the data and it will give access without the authentication so we are developing a system which gives the user better cloud environment. It will make that data permanently destructive which is stored by the cloud. With development of Cloud computing and popularization of mobile Internet, Cloud services are
becoming more and more important for people's life. People are more or less requested to submit or post some personal private information to the Cloud by the Internet. When people do this, they subjectively hope service providers will provide security policy to protect their data from leaking, so others people will not invade their privacy. As people rely more and more on the Internet and Cloud technology, security of their privacy takes more and more risks. On the one hand, when data is being processed, transformed and stored by the current computer system or network, systems or network must cache, copy or archive it. These copies are essential for systems and the network. However, people have no knowledge about these copies and cannot control them, so these copies may leak their privacy. On the other hand, their privacy also can be leaked via Cloud Service Providers (CSP's) negligence, hackers' intrusion or some legal actions. The SeDas system defines two new concepts, a self-destruct method object that is associated with each secret key part and survival time parameter for each secret key part. Aim of self-destructing system is to protect the user's data privacy. All the data and their copies become destructed after a user-specified time, without any user intervention. We focus on the related key distribution algorithm, which is Shamir's Secret Shares algorithm, which is used as the core algorithm to implement client (users) distributing keys in the object storage system. We use these methods to implement a safety destruct with equal divided key. In this SeDas, a system that meets this challenge through a novel integration of cryptographic techniques with active storage techniques based on T10 OSD standard. In Active Storage Framework, we use an object-based storage interface to store and manage the equally divided key.

2. Related Work

Self-destructing data concept is only for protecting the personal detail of the peoples. copies of data becomes inaccessible to the outsiders after the specified time duration. Besides, neither the sender nor the receiver can get the decryption key after the time-out.

The Washington's Vanish system which is vulnerable to "hopping attack" and "snifier attack", is a system for self-destructing data under cloud computing [1].

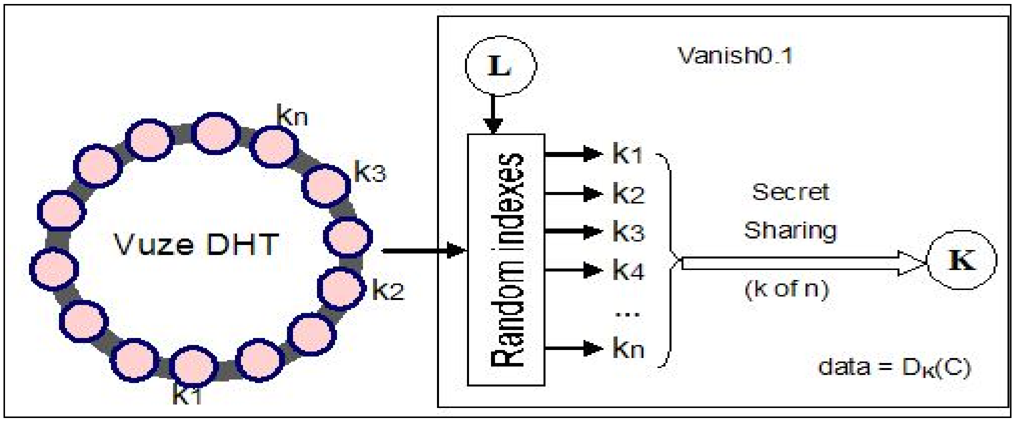


Figure 1: Encryption in Vanish

New scheme in this paper, called Safe Vanish, for preventing hopping attacks by way of extending the length range of the key shares, and did some improvement on the Shamir Secret Sharing algorithm implemented in the Original Vanish system. We present an improved approach against sniffing attacks by using the public key cryptosystem to protect from sniffing operations.

Wireless sensor networks technology is a rapidly growing domain, getting more and more credit in the area of civilian and military applications. In the same time with technological advancement, new and dangerous information security threats have emerged. In this paper we considered that a node self-destruction procedure must be performed as a final stage in the sensor node life cycle in order to assure the confidentiality regarding information like: network topology, type of measurement data gathered by sensors, encryption/authentication algorithms and key-exchange mechanisms, etc. that can be unveiled otherwise through reverse engineering methods. Our methodology relies on an eficient power monitoring scheme, based on combined in-network and predictive data, which discover the low battery nodes and initiate a self-destruction procedure for that nodes [2].

In the background of cloud, self-destructing data mainly aims at protecting the data privacy. All the data and its copies will become destructed or unreadable after a user-specified period, without any user intervention. Besides, anyone cannot get the decryption key after timeout, neither the sender nor the receiver. The Washington's Vanish system is a system for self destructing data under cloud computing, and it is vulnerable to hopping attack and snifier attacks. They propose a new scheme in this paper, called Safe Vanish, to pre- vent hopping attacks by way of extending the length range of the key shares to increase the attack cost substantially, and do some improvements[3].

In distributed systems, it is often needed to establish trust before entities interact together. This trust establishment process involves making each entity ask for some credentials from the other entity, which implies some privacy loss for both parties. We propose a model for achieving the right privacy-trust tradeoff in distributed environments. Each entity aims to join a group in order to protect its privacy. Interaction between entities is then replaced by interaction between groups on behalf of their members. Data sent between groups is saved from dissemination by a self-destruction process [4].

3. Proposed Work

We propose a system, a Self-Destructing Data System Based on Active Storage Frame-
Work and its application for cloud environment. This system explains about two new concepts, a self-destruct method object that is associated with each secret key part and survival time parameter for each secret key part. Self-destructing data mainly aims at protecting the user's data privacy. All the data and their copies become destructed or scribbled after a user-specified time, without any user intervention. We focus on the related key distribution algorithm, which is Shamir's Secret Shares algorithm, which is used as the core algorithm to implement users distributing keys in the object storage system. We use these methods to implement a safety destruct with equal divided key. In this SeDas, a system that meets this challenge through a novel integration of cryptographic techniques with active storage techniques based on T10 OSD standard. In Active Storage Framework, we use an object-based storage interface to store and manage the equally divided key.

3.1. Applying Software Engineering Approach

Software engineering (SE) is the application of a systematic, disciplined, quantifiable approach to the development, operation, and maintenance of software, and the study of these approaches; that is, the application of engineering to software. It is the application of engineering to software because it integrates significant mathematics, computer science and practices whose origins are in engineering. It is also defined as a systematic approach to the analysis, design, assessment, implementation, testing, maintenance and re-engineering of software, that is, the application of engineering to software. The Spiral Life Cycle Model is a type of iterative software development model which is generally implemented in high risk projects. It was first proposed by Boehm. In this system development method, we combine the features of both, waterfall model and prototype model. In Spiral model we can arrange all the activities in the form of a spiral.

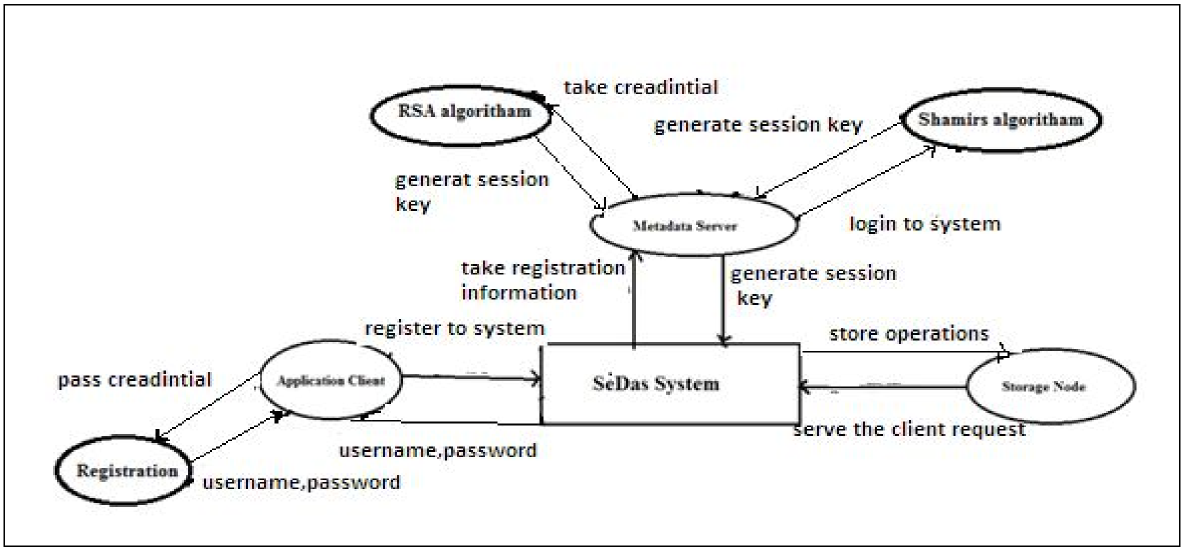
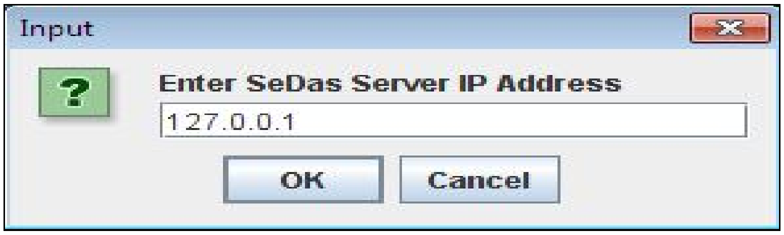


Figure 2: Flow of proposed system

This proposed system is one new system which will be more useful for the every field. This systems major goal is to protect the user as data privacy. And it can be achieved by using the Shamir's Secret share algorithm. This is the core algorithm in this system. The new key generated by the random function which is already in built in java. And that session key is divided into two parts by the Shamir Secret Share algorithm and at the time of validation the key is again validated by the Shamir's algorithm. The shamir's secret share algorithm is the most important technology which is used in this system all the major functions are done by this algorithm. Also this system uses the active storage devices such as SSD (Solid State Devices) and the HDDas(Hard Disk Drive)for the storage purpose.

4. Experimental Results

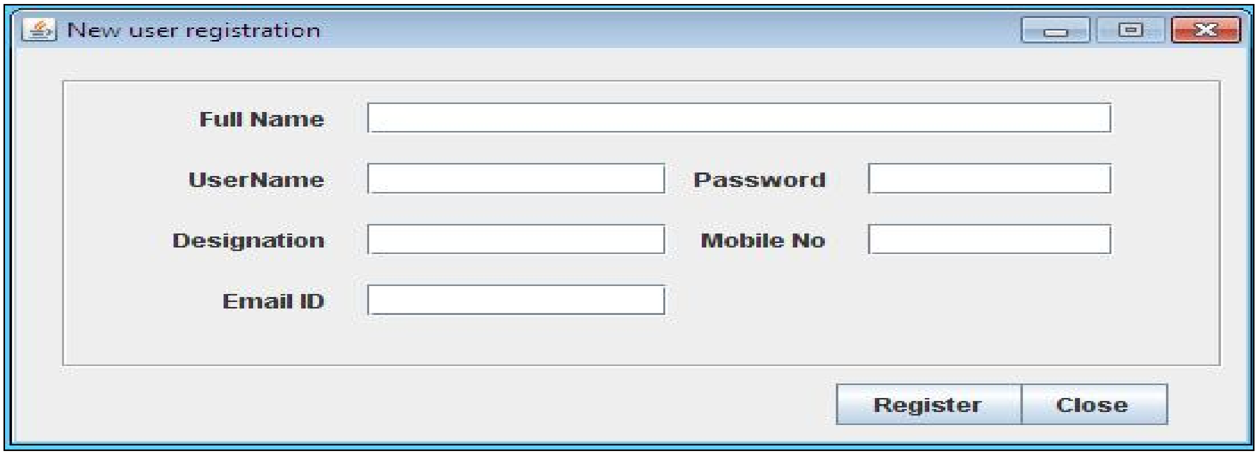

Input

Enter SeDas Server IP Address

127.0.0.1

Figure 3

This is screen after setting server IP address and connecting to server, it is asked for sedas IP address .


New user registration

Full Name

UserName

Password

Designation

Mobile No

Email ID

Figure 4

As soon as we enter sedas address, it is asked for new user registration with above detail so that sever can access this IP Adress next time automatically.

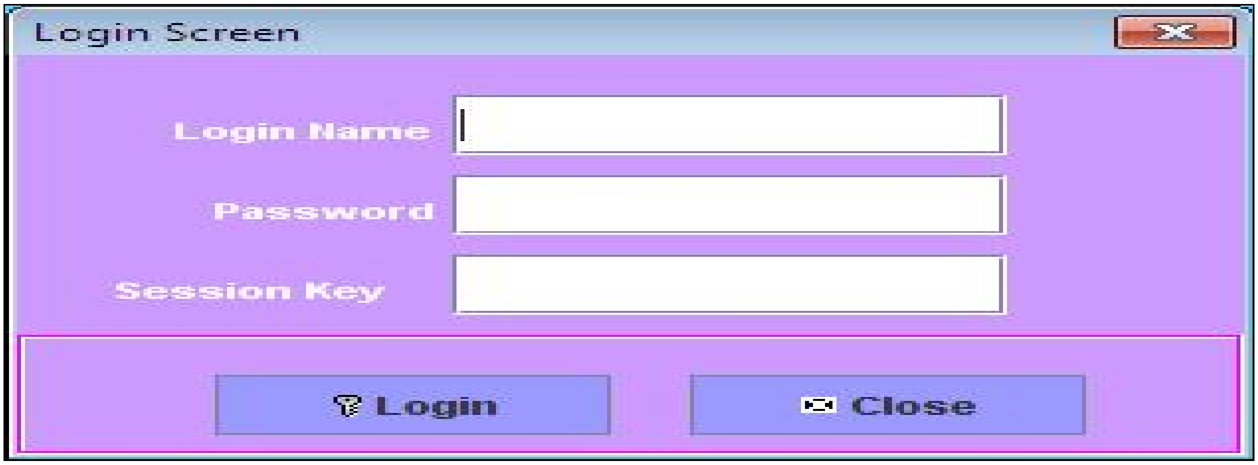
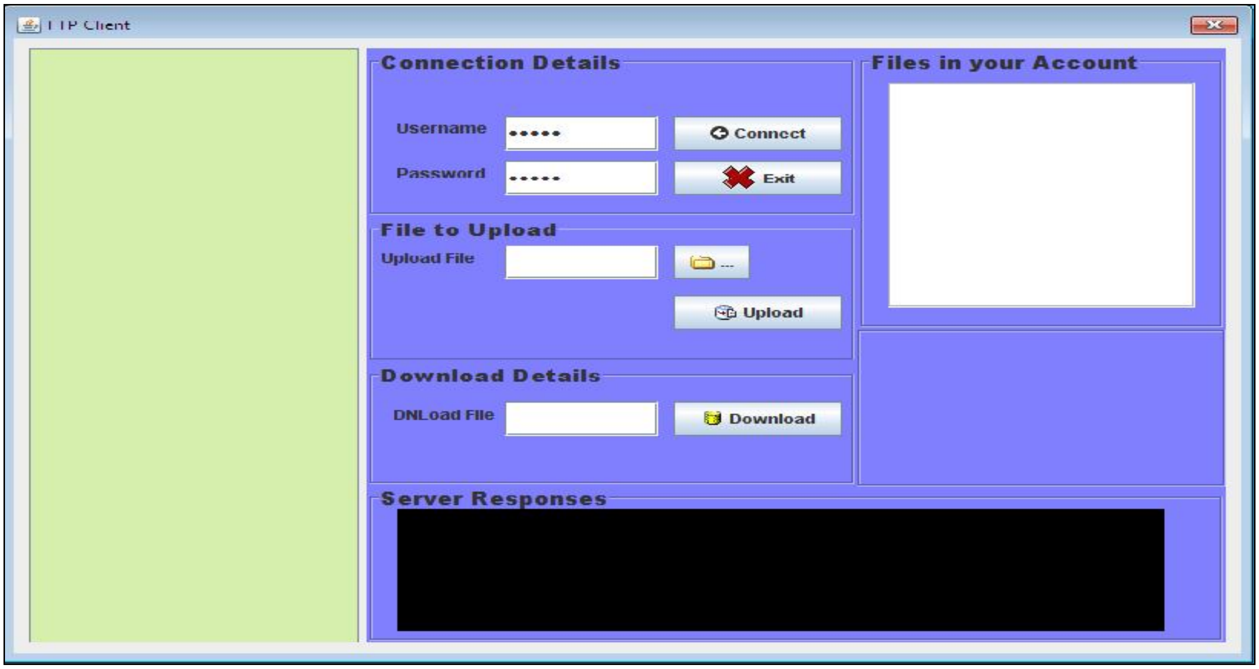


Figure 4

Before providing access server authenticate user with above required detail and then after it provides access.



Username •••••

Password •••••

Figure 5

This screen shows that user can upload new information to server once get access to server or he (user) can download his old files too.

5. Conclusion & Future Scope

Data privacy has become increasingly important in the Cloud environment. This paper introduced a new approach for protecting data privacy from attackers who retroactively obtain, through legal or other means, a user as stored data and private decryption keys. A novel aspect of our approach is the leveraging of the essential properties of active storage framework based on T10 OSD standard. We demonstrated the feasibility of our approach by presenting SeDas, a proof-of-concept prototype based on object-based storage techniques. SeDas causes sensitive information, such as account numbers, passwords and notes to irreversibly self-destruct, without any action on the user as part. Our measurement and experimental security analysis sheds insight into the practicability of our approach. Our plan to release the current SeDas system will help to provide researchers with further valuable experience to inform future object-based storage system designs for Cloud services.

This SEDAS system have the very broad concept in this paper we are implementing the only shamir's secret share algorithm but in future this SEDAS system can make so much improvements. Such as this can be used as a security environment. This will also do some modification in the no of shares presents.

6. References

1. Cloud Computing Technology and Science (Cloud Com), 2010 IEEE Second International Conference on Safe Vanish: An Improved Data Self-Destruction for Protecting Data Privacy".
2. Applied Computational Intelligence and Informatics, 2009. SACI '09. 5th International Symposium on: Energy-driven methodology for node self-destruction in wireless sensor networks"
3. Innovations in Information Technology, 2008. IIT 2008. International Conference on : " Trust-privacy tradeo_s in distributed systems"
4. L. Qin and D. Feng, active storage framework for object-based storage device,^O in Proc. IEEE 20th Int. Conf. Advanced Information Networking and Applications (AINA), 2006.
5. Y. Zhang and D. Feng, ^On active storage system for high performance computing in Proc. 22nd Int. Conf. Advanced Information Networking and Applications (AINA), 2008, pp. 64451.
6. T. M. John, A. T. Ramani, and J. A. Chandy, ^ Octive storage using object-based devices, in Proc. IEEE Int. Conf. Cluster Computing,2008,
7. A. Devulapalli, I. T. Murugandi, D. Xu, and P. Wycko_, 2009,Design of an intelligent object-based storage device [Online].
8. S. W. Son, S. Lang, P. Carns, R. Ross, R. Thakur, B. Ozisikyilmaz, W.-K. Liao, and A. Choudhary, ^ Onabling active storage on parallel I/O software stacks,^O in Proc. IEEE 26th Symp.