ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)
Vol. 4, Issue 2 (Apr. - Jun. 2016)
International Journal of Advanced Research in Computer Science & Technology (IJARCST 2016)

Well-Organized Key for Trait Based Encryption and Decryption using Toolkit for File Protection

[I]P. Rajapandian, [II]P. Logaiyan, [III]C. Samundhiswari
[I]Assistant Professor [Sr. Gr.] & Head, [II]Assistant Professor [Sr. Gr.], [III]Final year Student
[I,II,III]Dept. of M.C.A., Christ College of Engineering and Technology, Pondicherry, India

Abstract
BlowFish encryption algorithm provides a mechanism for complex access control over encrypted data. It is used to secure and encrypting file system on Android operating system and optimize the performance using certified encryption algorithm BlowFish provided in OPENSSL libraries. This paper presents EncFS which is a FUSE (File system in USErspace) based file-system offering encryption file system to protect the removable and persistent storage on heterogeneous smart gadget devices running the Android platform. In proposed methodology, the data at rest including physical partition on the device and removable storage card is encrypted using user provided password. The encrypted file system is mounted only after successful password verification with user at system boot up.

Keywords
Encryption, Decryption, Data Privacy, Blowfish, Secret keys

I. Introduction

Mobile computing is human–computer interaction by which a computer is expected to be transported during normal usage. Mobile computing involves mobile communication, mobile hardware, and mobile software. Communication issues include ad hoc and infrastructure networks as well as communication properties, protocols, data formats and concrete technologies. Hardware includes mobile devices or device components. Mobile software deals with the characteristics and requirements of mobile applications. Many commercial and government field forces deploy a ruggedized portable computer with their fleet of vehicles. This requires the units to be anchored to the vehicle for driver safety, device security, and ergonomics. Rugged computers are rated for severe vibration associated with large service vehicles and off-road driving and the harsh environmental conditions of constant professional use such as in emergency medical services, fire, and public safety.

Mobile security or mobile phone security has become increasingly important in mobile computing. It is of particular concern as it relates to the security of personal information now stored on the smartphone. More and more users and businesses use smartphones as communication tools but also as a means of planning and organizing their work and private life. Within companies, these technologies are causing profound changes in the organization of information systems and therefore they have become the source of new risks. Indeed, smartphones collect and compile an increasing amount of sensitive information to which access must be controlled to protect the privacy of the user and the intellectual property of the company. All smartphones, as computers, are preferred targets of attacks. These attacks exploit weaknesses related to smartphones that can come from means of communication like SMS, MMS, wi-fi networks, and GSM. There are also attacks that exploit software vulnerabilities from both the web and operating system.

Finally, there are forms of malicious software that rely on the weak knowledge of average users.Different security counter-measures are being developed and applied to smartphones, from security in different layers of software to the dissemination of information to end users. There are good practices to be observed at all levels, from design to use, through the development of operating systems, software layers, and downloadable apps.

Android is popular with technology companies which require a ready-made, low-cost and customizable operating system for high-tech devices. Android's open nature has encouraged a large community of developers and enthusiasts to use the open-source code as a foundation for community-driven projects, which add new features for advanced users or bring Android to devices which were officially, released running other operating systems. The operating system's success has made it a target for patent litigation as part of the so-called "smartphone wars" between technology companies.

Wireless data connections used in mobile computing take three general forms so. Cellular data service uses technologies such as GSM, CDMA or GPRS, 3G networks such as W-CDMA, EDGE or CDMA2000. And more recently 4G networks such as LTE, LTE-Advanced. These networks are usually available within range of commercial cell towers. Wi-Fi connections offer higher performance, typical range of 100 feet indoors and up to 1000 feet outdoors. Satellite Internet access covers areas where cellular and Wi-Fi are not available and may be set up anywhere the user has a line of sight to the satellite's location, which for satellites in geostationary orbit means having an unobstructed view of the southern sky. Some enterprise deployments combine networks from multiple cellular networks or use a mix of cellular, Wi-Fi and satellite.

When using a mix of networks, a mobile virtual private network (mobile VPN) not only handles the security concerns, but also performs the multiple network logins automatically and keeps the application connections alive to prevent crashes or data loss during network transitions or coverage loss.

II. Related work

The Complex fat operators are important contributors to the efficiency of specialized hardware. This paper introduces two new techniques for constructing efficient fat operators featuring up to dozens of operations with arbitrary and irregular data and memory dependencies. These techniques focus on minimizing critical path length and load-use delay, which are key concerns for irregular computations. Selective Depipelining (SDP) is a pipelining technique that allows fat operators containing several, possibly dependent, memory operations. SDP allows memory requests to operate at a faster clock rate than the data path, saving power in the datapath and improving memory performance. Cachelets are small, customized, distributed L0 caches embedded in the datapath to reduce load-use latency. We apply these techniques

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

to Conservation Cores(c-cores) to produce coprocessors that accelerate irregular code regions while still providing superior energy efficiency. On average, these enhanced c-cores reduce EDP by 2× and area by 35% relative to c-cores. They are up to 2.5× faster than a general-purpose processor and reduce energy consumption by up to 8× for a variety of irregular applications including several SPECINT benchmarks [3].

We are coming into an interesting era for techniques design—one motivated by datacentric processing. A latest review from the School of San Paul approximated that, cautiously, business server techniques have prepared and provided more than 9 zettabytes of details in 2008 (where 1 zettabyte ¼ 1021 bytes) this number is estimated to double every two decades. Wal-Mart web servers, for example, handle more than 1 million customer dealings every hour, providing data source approximated in several petabytes. High-performance processing techniques working with the Huge Hadron Collider narrow through approximately one petabyte of details per second and still produce 15 petabytes a year after several levels of details selection. Each day, Facebook or myspace functions on nearly 100 terabytes of customer log details and several hundred terabytes of customer pictures; in the same way, 48 hours of video content is submitted every minute on YouTube. On one side, the capability to gather and procedure considerable amounts of new details can drive medical developments, new company procedure optimizations, and day-to-day developments in our personal lives. Recent data-centric programs for customized genome sequencing, real-time styles from company statistics, social-network-based suggestions, and so on illustrate this potential. But however, this detail is also creating a variety of new problems. In particular, the growth in details produced is outpacing the developments in the cost and solidity of storage technological innovation. Also, perhaps even more important, our capability to procedure the details to draw out significant, workable ideas is considerably lagging our capability to gather and store details. Given these difficulties and possibilities, it is important to reconsider how we design future data-centric techniques. Simultaneously, technology inflections such as the improved adopting of non-volatile remembrances, visual emails, multicores, and heterogeneous processing all provide a unique chance of an end-to-end upgrade of data-centric alternatives across both software and components. Here, we talk about latest computer structure and techniques analysis printed with such redesigns, culling out cross-cutting guidelines across these tasks that recommend analysis possibilities for the wider community [1].

In this paper we set up essential restrictions to the advantage of system programming with regards to power and throughput in multi-hop Wi-Fi systems. Thereby we follow two well approved circumstances in the field individual multicast period and several unicast classes. Most of our results apply to irrelevant Wi-Fi system and are, in particular, not asymptotic in kind. In conditions of throughput and power preserving we confirm that the obtain of system programming of only one multicast period is at most a continuous aspect. Also, we present a lower limited on the expected number of signals of several unicast classes under an irrelevant system programming. We recognize circumstances for which the system programming obtain for power preserving becomes amazingly close to 1, in some cases even exactly 1, corresponding to no advantage at all. Remarkably, we confirm that the obtain of system programming with regards to transportation potential is surrounded by a continuous aspect _ in any irrelevant Wi-Fi system and for all conventional route models. This shows that the conventional range on the transportation potential do not change more than continuous aspectif we employ system programming. As a corollary, we find that the obtain of system programming on the throughput of extensive homogeneous Wi-Fi systems is asymptotically surrounded by a continuous. Note that our result is more general than the previous work and it is obtained by a different technique. In summary, we show that contrary to wired systems, the system programming obtain in Wi-Fi systems is restriction by essential restrictions [4].

Our analysis concentrates on analogue CMOS routine style with focus on high regularity and high speed internet tour. With the pattern of program incorporation in mind, we try to create new routine methods that allow the next steps in program incorporation in nanometer CMOS technological innovation. Our analysis financing comes from industry, as well as from government companies. We aim to find essential alternatives for realistic issues of incorporated tour noticed in industrial Rubber technological innovation. CMOS IC technological innovation is determined by maximum cost and efficiency of digital tour and is certainly not enhanced for nice analogue actions. As analogue developers, we do not have the impression of being able to change CMOS technological innovation, so we have to "live with it" and fix the issues by style. In this article several illustrations will be proven where challenging analogue actions, such as disturbance and distortions, can be handled with new routine style methods. These routine methods are designed in such a way that they do benefit from today's technological innovation and thus allow further incorporation. This way we can enhance various analogue foundations for Wi-Fi, wire-line and visual interaction [2].

III. Existing System

A major obstacle is that there is a serious lack of National Institute of Standards (NIST) approved encryption algorithms on these commercially available smart gadgets. Much less common is the existence of any encryption techniques that can pass the strong government validation process in place for any computing device to be used in an adversarial environment. Also, the expectation for each individual application to support encryption runs into the key management problem and the other applications in the system can potentially gain access to the key and render the encryption useless. Therefore, there is a need for a practical approach to build common security libraries that operate at the operating system level and provide strong encryption. This system has to be ubiquitous and integrate into the ecosystem of smart gadgets with minimal maintenance and installation cost.

A. Disadvantages of Existing system

- Encryption however comes at a significant performance cost.
- On smart gadgets where resources, like the battery, are very limited, it is important to keep a low footprint on such solutions.

IV. Proposed System

In proposed methodology, EncFS (FUSE-based file-system) is used to encrypt data in the server at rest including physical partition on the device and removable storage card using user provided password. To have EncFS support Android with the appropriate space, three major components are required: kernel FUSE library support, user space libfuse, and EncFS binaries. To make an encryption file-system work on Android, a modified bootstrapping

process and password login is planned to be integrated into the operating system framework.

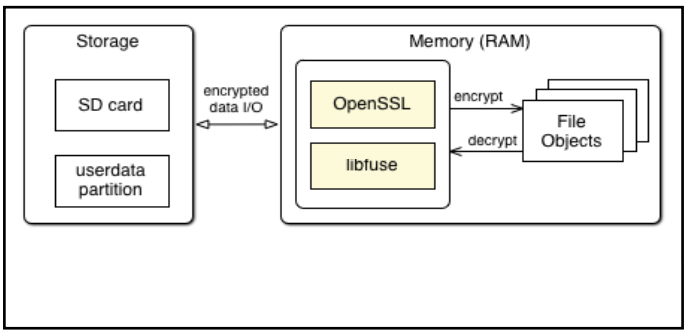

Fig. 1 : Abstraction of Encryption File system on Android

When the system is completely booted up, user is asked for password. If the password provided by the user is valid, the encrypted file system is mounted on /data mount point. It stores the encrypted data in a separate directory and mounts it over / data partition when the user supplies the password. If the mount is performed successfully, the launcher will call a dedicated native program to soft reboot Android Dalvik environment and the user is presented with his encrypted user data partition, decrypted into the memory transparently. The user has limited number of login attempts. After exceeding number of attempts, all the encrypted data is erased

A. Advantages of Proposed system

- To achieve better performance, this paper proposes to optimize the EncFS and use BlowFish which is symmetric block cipher with a 64-bit block size and a variable key length from 32 bits up to 448 bits.
- On analysing the performance for persistent storage protection using encryption on smart gadget devices.

B. Module Explanation

1. Registration

This module explains the design and implementation of user registration via web based services. This module wills also communication established between client and server based web service application.

2. User

A user can upload/ download file. When uploading file Blowfish, and AES schemes are used to encrypt data & signature is included to lock that data and when downloading the files inversely Blowfish and AES are used to decrypt data & signature is used to unlock the file.

3. Network Module

Server - Client computing or networking is a distributed application architecture that partitions tasks or workloads between service providers is uploading information (servers) and service requesters will be downloading information, called clients. Often clients and servers operate over a computer network for three ways of cryptography standard techniques apply. A server machine is a high-performance host that is running one or more server programs which share its resources with clients. A client also shares any of its resources; Clients therefore initiate communication sessions with servers which await incoming requests.

4. Blowfish Algorithm

Blowfish Algorithm Blowfish is a symmetric block cipher algorithm. It uses the same secret key to both encryption and decryption of messages. The block size for Blowfish is 64 bits; messages that aren't a multiple of 64-bits in size have to be padded. It uses a variable –length key, from 32 bits to 448 bits. It is appropriate for applications where the key is not changed frequently. It is considerably faster than most encryption algorithms when executed in 32-bit microprocessors with huge data caches.

5. Verification Module

In the verification module, the input signature is verified with the server authenticated signatures. And results will be displayed based on the verification. An automatic signature verifier should assess whether a questioned signature is an authentic signature normally used by the reference writer. These parameters were evaluated with different classifiers such as nearest neighbour.To make an encryption file-system work on Android, a modified bootstrapping process and password login is planned to be integrated into the operating system framework.

V. Conclusion and Future Enhancement

In this paper we used to protect users' data privacy is a central question of cloud storage. With more mathematical tools, cryptographic schemes are getting more versatile and often involve multiple keys for a single application. In this paper, we consider how to "compress" secret keys in public-key cryptosystems which support delegation of secret keys for different ciphertext classes in cloud storage. No matter which one among the power set of classes, the delegate can always get an aggregate key of constant size. Our approach is more flexible than hierarchical key assignment which can only save spaces if all key-holders share a similar set of privileges. A limitation in our work is the predefined bound of the number of maximum ciphertext classes. In cloud storage, the number of ciphertexts usually grows rapidly. So we have to reserve enough ciphertext classes for the future extension. Otherwise, we need to expand the public-key as the parameter can be downloaded with ciphertexts, it would be better if its size is independent of the maximum number of Ciphertext classes. In cloud storage, the number of ciphertexts usually grows rapidly. So we have to reserve enough Ciphertext classes for the future extension. It would be better if its size is independent of the maximum number of Ciphertext classes. On the other hand, when one carries the delegated keys around in a mobile device without using special trusted hardware, the key is prompt to leakage, designing a leakage-resilient cryptosystem yet allows efficient and flexible key delegation is also an interesting direction.

References

[1] *G. Venkatesh et al., "Conservation Cores: Reducing the Energy of Mature Computations," Proc. 15th Int'l Conf. Architectural Support for Programming Languages and Operating Systems, ACM Press, 2010, pp. 205-218.*

[2] *R. Dennard et al., "Design of Ion-Implanted MOSFET's with Very Small Physical Dimensions," IEEE J. Solid-State Circuits, vol. 9, no. 5, 1974, pp. 256-268.*

[3] *J. Sampson et al., "Efficient Complex Operators for Irregular Codes," Proc. 17th IEEE Int'l Symp. High Performance Computer Architecture, IEEE Press, 2011, pp. 491-5021999.*

[4] *M. Fiore, F. Mininni, C. Casetti, and C.F. Chiasserini, "To*

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

Cache or Not to Cache?" Proc. IEEE INFOCOM, pp. 235-243, 2009.

[5] S. Jahid, P. Mittal, and N. Borisov, "Easier: encryption-based accesscontrol in social networks with efficient revocation," in Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, ser. ASIACCS '11. New York, NY, USA: ACM, 2011, pp. 411–415.

[6] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based datasharing with attribute revocation," in Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, ser. ASIACCS '10. New York, NY, USA: ACM, 2010, pp. 261–270.

[7] J. Li, C. Jia, J. Li, and X. Chen, "Outsourcing encryption of attribute-based encryption with mapreduce," in Proceedings of the 14th International Conference on Information and Communications Security, ser. ICICS'12. Berlin, Heidelberg: Springer-Verlag, 2012, pp. 191–201.

[8] J. A. Akinyele, C. Garman, I. Miers, M. W. Pagano, M. Rushanan,M. Green, and A. D. Rubin, "Charm: a framework for rapidly prototyping cryptosystems," Journal of Cryptographic Engineering, vol. 3, no. 2, pp. 111–128, 2013.

Author Profile

P.Rajapandian is an Assistant Professor[Sr. Gr.] & Head of Master of Computer Applications in Christ College of Engineering and Technology affiliated to Pondicherry University, India.

P. Logaiyan is an Assistant Professor [Sr. Gr.] of Master of Computer Applications in Christ College of Engineering and Technology affiliated to Pondicherry University, India.

C. Samundhiswari is a final year Student of Master of Computer Applications in Christ College of Engineering and Technology affiliated to Pondicherry University, India.