Symmetry **2015**, *7*, 935-948; doi:10.3390/sym7020935

OPEN ACCESS

symmetry

ISSN 2073-8994

www.mdpi.com/journal/symmetry

Article

Design of a Distributed Personal Information Access Control Scheme for Secure Integrated Payment in NFC

Jungho Kang [1], Jong Hyuk Park [2] and Sangkee Suk [2,*]

[1] Department of Computing, Soongsil University, 402 Information Science Building, 369 Sangdo-Ro, Dongjak-Gu, Seoul 156-743, Korea; E-Mail: kjh7548@naver.com

[2] Department of Computer Science and Engineering, Seoul National University of Science and Technology, Gongneung 2-dong, Nowon-gu, Seoul 139-743, Korea; E-Mail: jhpark1@seoultech.ac.kr

***** Author to whom correspondence should be addressed; E-Mail: sksuk@seoultech.ac.kr; Tel.: +82-2-970-6708; Fax: +82-2-977-9441.

Academic Editor: Young-Sik Jeong

Received: 16 January 2015 / Accepted: 27 May 2015 / Published: 2 June 2015

Abstract: At the center of core technologies for a future cyber world, such as Internet of Things (IoT) or big data, is a context-rich system that offers services by using situational information. The field where context-rich systems were first introduced is near-field communication (NFC)-based electronic payments. Near-field Communication (NFC) integrated payment services collect the payment information of the credit card and the location information to generate patterns in the user's consumption or movement through big data technology. Based on such pattern information, tailored services, such as advertisement, are offered to users. However, there is difficulty in controlling access to personal information, as there is a collaborative relationship focused on the trusted service manager (TSM) that is close knit to shared personal information. Moreover, in the case of Hadoop, among the many big data analytical technologies, it offers access control functions, but not a way to authorize the processing of personal information, making it impossible to grant authority between service providers to process information. As such, this paper proposes a key generation and distribution method, as well as a secure communication protocol. The analysis has shown that the efficiency was greater for security and performance compared to relation works.

Keywords: access control; distributed file system; NFC eco-system; personal-information; Hadoop; future cyber world

1. Introduction

Information technologies that can be used in the future cyber world, such as IoT, big data, cloud computing and smart cars, are all based on a context-rich system. A context-rich system is a technology that offers services tailored to new situation information and is based on big data technology [1]. The first field to have such context-rich technology applied was near-field communication (NFC) integrated payment services, which is expected to be the basic electronic payment technology in the future cyber world.

NFC integrated payment services transfer credit card information, mileage card information and membership information stored on a smart phone to the POS device all at one time using NFC technology and allow this to be confirmed through an application [2].

When the NFC integrated payment services are used, the credit card company collects the payment information, the mobile network operation collects the location information, the mileage company collects the item information and the coupon provider collects personal information on a constant basis. Such information is then analyzed to generate information on the user's consumption pattern, which is then used to offer tailored advertisement or coupons to the user [2–6].

Such a payment system not only processes simple personal information, but also generates and processes sensitive information related to the user's lifestyle, consumption and movement, and therefore, secure access control to such information is needed. Moreover, since various corporations are in a collaborative network sharing personal information, access control needs to be provided by the group.

Given that multiple corporations collect massive amounts of information in various forms and formats in real time and analyze them to provide services, NFC integrated payment services can be seen as based on big data. However, when Hadoop, one of the major big data technologies, is applied to NFC integrated payment services, the access authorization technology provided by Hadoop cannot control the processing of personal information in the NFC eco-system, which is a close meshed network centered on a trusted service manager (TSM) [2,3]. In addition, Hadoop has vulnerabilities in setting authorization for files, disclosure of session keys and replay attacks.

As such, in this paper, the characteristics of the NFC eco-system where NFC integrated payment services are provided will be taken into account to propose a measure of secure access control when there is sensitive personal information, such as that concerning the user's lifestyle, consumption and movement patterns.

2. Near-Field Communication

NFC is a non-contact wireless communication technology capable of exchanging data at close quarters. NFC operates at a frequency of 13.56 MHz, and the communication range is about 10 cm or less. Because it uses RF, it can be categorized as a type of radio frequency identification (RFID). The

biggest difference between the two technologies is that NFC allows peer-to-peer (P2P) communication. NFC operates in three modes, as seen in Table 1 [2,7].

Table 1. Characteristics of each near-field communication (NFC) operation mode.

Operation Mode	Characteristics	Applicable Services
P2P	NFC devices can exchange data in peer-to-peer mode	Exchange of electronic business cards P2P payment Exchange of data between devices
Read/Write Reader	A reader that allows both reading and writing; the NFC device operates to read NFC tags	Smart posters Tourist information Simple NFC
Card Emulation	NFC devices can exchange data with an external reader, as the NFC tag	Public transport cards Mobile credit cards

2.1. NFC Integrated Payment

When an NFC integrated payment system is used, the payment information, location information, history of coupon usage and mileage information are accumulated in the TSM. Pattern information refers to the information that has been processed from the payment pattern, movement pattern and lifestyle of the user. TSM analyzes pattern information to offer tailored services, by sending the information to the service provider [7,8].

At present, the NFC integrated payment system offered by Google is a type that uses pattern information. The TSM corporation that participates in Google Wallet services is First Data, which serves as a medium for transmitting information. Google processes information to generate pattern information and manages the SE (Secure Element) and application. In regards to payment, Citi Bank is a partner, and a variety of financial institutions, credit card companies, mobile service providers and merchants collect personal information [8].

2.2. Trusted Service Management

A trusted service manager (TSM) is a technology that emerged to offer secure mobile financial services. In NFC services, too, it serves as a market and technology mediator through security management services [7,8].

TSM has access authority to SE fields and is at the center where data generated by NFC services are collected. TSM controls the entire process of NFC services. It manages the application, issuance and suspension of the means by which the service is used and also manages the service provider's account and NFC device. For example, the service usage means in NFC payment services can be a mobile credit card.

The role of TSM can be understood through a comparison of the following two images. Figure 1 shows the structure of how information was transmitted before TSM was adopted between MNO (Mobile Network Operation) and service providers. Figure 2 shows the structure after TSM was adopted between MNO (Mobile Network Operation) and service providers.

The concept of TSM was first introduced by Global System for Mobiles Association (GSMA), after which, together with the European Payments Council (EPC), the eco-system of mobile contactless payments (MCP) based on universal integrated circuit card (UICC) further defined the role of TSM.

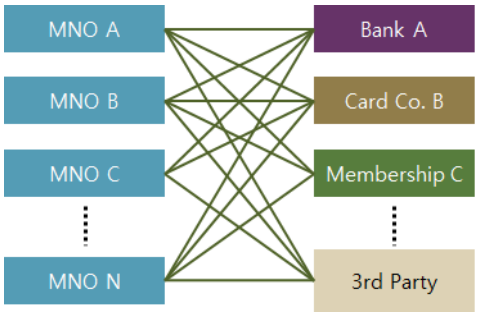

Figure 1. Structure of information transmission before the trusted service manager (TSM) was adopted.

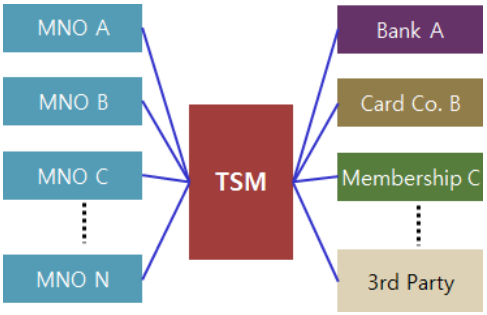

Figure 2. Structure of information transmission after the TSM was adopted.

For example, in a model such as Google Wallet services, all data related to payment services are concentrated in the TSM. Google uses such data to provide tailored services to its users. That is, the role of TSM is very important from the perspective of personal information [8].

3. Hadoop

Hadoop is an open source framework of Apache that allows massive amounts of data to be stored, distributed and analyzed. Originally, it was developed by Mike Cafarella and Douglas Cutting, the creators of Apache Lucene, to support distributed processing in Nutch, an open source web search engine [9–11].

Hadoop was realized by benchmarking Google's Google File System and can be said to be the core technology to provide context-rich services in NFC integrated payment.

The Hadoop distributed file system adopted Kerberos and a token system for security reasons, but there are weaknesses, such as the issue of setting authorization for the files, sharing one key, replay attacks of the block access token and vulnerability against masked attacks [9,10,12,13].

3.1. No Support for Setting File Authorization

The Hadoop distributed file system is designed to operate in a general use computer. Most distributed file system of Hadoop operates in Linux/Unix operating systems. The Hadoop distributed file system does not have a function of setting authorization for files in itself, but uses the function that is provided by the operating system. Since such methods cannot be applied to the security functions of Kerberos or token systems, if the user has been authorized through Kerberos, his authorization is not confirmed separately when files are accessed [14].

3.2. Issues with the Usage and Exchange of Keys

For encrypted communication between the client node, name node and data node in the Hadoop distributed file system, a key must be exchanged in advance. However, there are issues with how the key is shared in advance or with the shared key itself [15].

The name node and all data nodes share one secret key. This secret key is transmitted when the data node is first registered with the name node. When the key is changed, the name node, through the heart beat that is regularly transmitted by the data node, transmits the changed key. If the attacker disguises himself as a data node and registers with the name node or intercepts the heart beat and the key value is disclosed, the attacker can use the acquired key to generate a block access token. That is, the attacker can access the block of the data node to acquire data.

Moreover, in the PKI (Public Key Infrastructure) system, one client shares a public key with all data nodes, and one data node has to share the public key with all clients and also store the public keys of other data nodes.

3.3. Replay Attacks and Disguised Attacks

The biggest problem with the block access token used in Hadoop is that it does not have a security measure other than comparing the token ID with the token authority, which is the hash value to verify the integrity of the token ID. That is, even when someone other than the actual owner of the clock access token transmits it, there is no process to verify it, and the token, once issued, can be re-used several times during the valid period. This allows the attacker to conduct a replay attack after acquiring the token [12,13,16].

At present, the Hadoop distributed file system shares a secret key between the name node and the client. The user encrypts the transmitted data using this secret key to acquire the ticket or block access token, then sends it to the server from which he aims to be certified. When the integrity of the token is verified, the user is confirmed as an approved user. Since the user cannot know what the content of the block access token or ticket is, from the user's perspective, there is no way to know whether the transmitted ticket or block access token was transmitted by a normal name node. In addition, since there is no way for the data node to verify the user either, there is no way to confirm whether the transmitted file was sent by a normal data node or was a malicious file sent by an attacker [17].

4. Proposed Scheme

The proposed distributed personal information access control scheme consists of a service provider, TSM and pattern information management (PIM). The TSM distributes the keys and verifies in accordance with information mediation and authorization, while PIM refers to a distributed file system like Hadoop. In designing a Hadoop-based PIM, the PIM is composed of the name node and data node. The name node functions as the manager of thousands of data nodes, saves files in the data node and performs tasks by receiving requests from users. Actual files are saved in the data nodes.

The proposed security scheme only regulates the communication between the service provider and PIM and assumes that the session key based on the public key has been generated and distributed before the initial communication. Moreover, Service Provider 1 and Service Provider 2 are in a collaborative

relationship. Service Provider 2 only has the authority to view personal information and pattern information, while Service Provider 1 is assumed to have the authority to revise personal information, as well. The terms and symbols used in the proposed security protocol are shown in Table 2.

Table 2. The terms and symbols used in proposed security protocol.

Cert	Certification
Sign	Digital Signature
E_{PUB} and D_{PUB}	Encryption and Decryption by Public Key
E_{PRI} and D_{PRI}	Encryption and Decryption by Private Key
NN	Name Node
DN	Data Node
SP	Service Provider
Req and Res	Request and Response
N_i	Random Number
A_B_SK_i	i-th Session Key between A to B
PI_A_MK_i	i's Personal Information Modification Key
PI_A_AK_i	i's Personal Information Access Key
h()	Hash Function

4.1. Key Generation and Management Scheme

4.1.1. The Process of Session Key Generation

All communication processes go through verification of the certification, generation of a session key and encryption using the session key. The process of generating the seed key, which is the session key used between all entities, is as seen in Figure 3.

The service provider (SP), TSM, name node and data node generate a random number to create the seed key and verify each other through a certification. After verification, the SP, TSM, name node and data node transmit a random number through the public key and generate a seed key for the generation of a session key. Lastly, for the SP and TSM to communicate with each other, the seed key generated by sharing the value of the random number is transmitted to the TSM for verification. When transmitted, it is encrypted using the public key of the TSM and has the signature of the SP attached. The TSM, name node and data node also transmit and verify the seed key in the same manner.

4.1.2. The Process for Generating the Key for the Authorization of Access to and Modification of Personal Information and Pattern Information

The key to handling personal information and pattern information has different authorizations for each SP and is designed based on the secret sharing method. The process of generating and distributing the authorization key for access to and modification of personal information and pattern information is as seen in Figure 4. All keys are generated in the TSM, and SP1 receives the key with the authorization to revise personal information and pattern information. SP2 receives only the key for viewing authorization.

The TSM selects "PI_A_MK_S" as the secret constant in the polynomial equation and selects the four points that pass through Formula (1), which are "PI_A_MK_TSM", "PI_A_MK_SP1",

"PI_A_MK_NN" and "PI_A_MK_DN". At this point, "PI_A_MK_SP1" becomes the key with the authorization to revise personal information and pattern information for SP1 and is encrypted into a session key to be transmitted to SP1. The TSM deletes "PI_A_MK_S" and only stores "PI_A_MK_TSM". It encrypts "PI_A_MK_NN" and "PI_A_MK_DN" as a session key and transmits it to the name node (NN) and data node (DN). At the same time, TSM transmits to the DN the hashed "PI_A_MK_S".

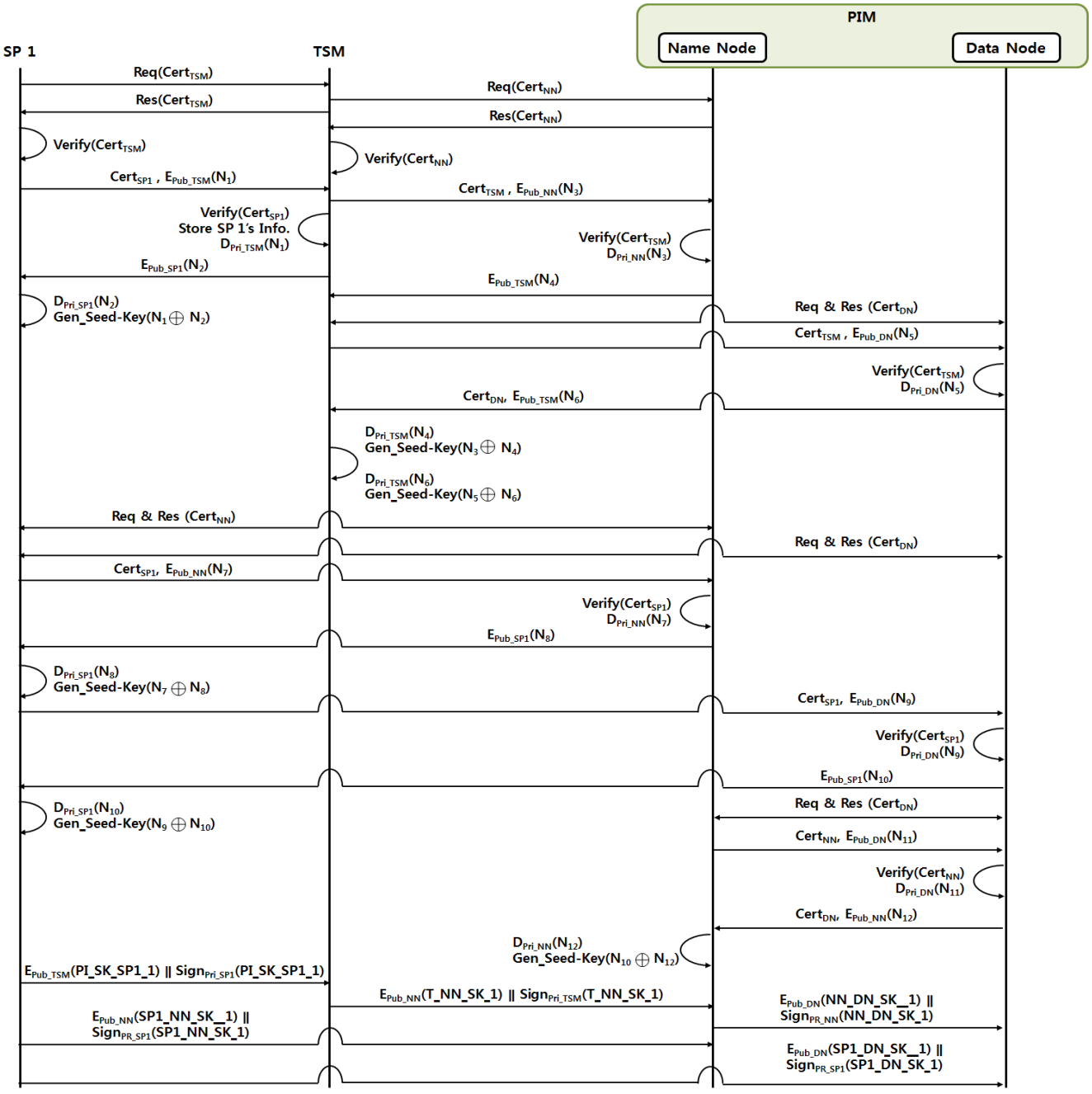

Figure 3. Session key generation protocol. PIM, pattern information management.

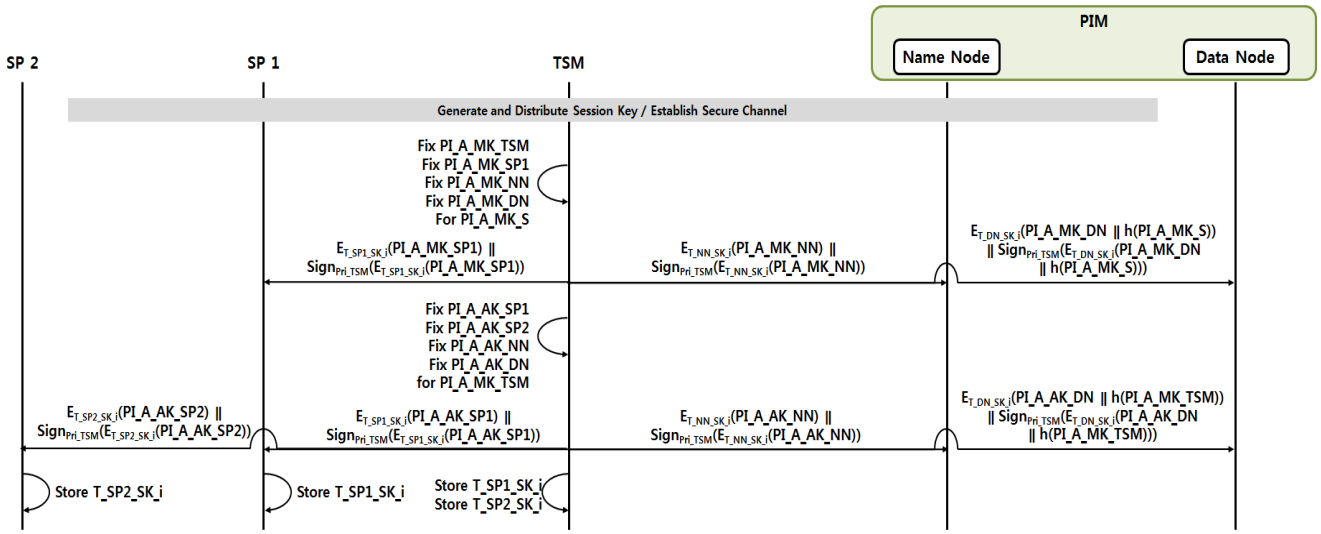

Figure 4. Authorization key management protocol.

$$Y = aX^3 + bX^2 + cX + PI\_A\_MK\_S \quad (1)$$

$$Y = aX^2 + bX + PI\_A\_MK\_TSM \quad (2)$$

After the key for the authorization for modification is generated and transmitted, the TSM generates simple viewing keys for personal information and pattern information. TSM creates Formula (2) using "PI_A_MK_TSM" as a secret constant and selects the four points that pass through Formula (2), which are "PI_A_AK_SP1", "PI_A_AK_SP2", "PI_A_AK_NN" and "PI_A_AK_DN". At this point, "PI_A_AK_SP1" and "PI_A_AK_SP2" become the simple viewing key for personal information and pattern information for SP1 and SP2. They are encrypted into a session key to be transmitted to SP1 and SP2. The TSM deletes "PI_A_MK_TSM" and encrypts "PI_A_AK_NN" and "PI_A_AK_DN" into a session key to transmit it to the NN and DN. The last session keys to be used are stored in the TSM, and the TSM transmits to the DN the hashed "PI_A_MK_TSM".

4.2. Transmission and Access Scheme for Personal Information and Pattern Information

4.2.1. The Process of Transmitting Personal Information

Figure 5 shows the protocol of storing in PIM the personal information that SP1 has collected.

SP1 divides a single file to be saved by a unit of 64 MB, a block size. Then, SP1 transmits a file name, the size, the number of divided blocks and owner information of the file to the TSM; whereas it transmits the information above to the name node. The name node saves the file information in the name space and allocates the data node to notify to the TSM. The TSM retransmits the data node information to SP1; whereas SP1 forms a secure channel with the data node in the same way as is shown in the Figure 3. SP1 implements the first stage of encryption of the collected personal information using the session key with the DN, then double-encrypts it using the session key with the TSM before it transmits to the TSM. The TSM verifies the packet that was received through the signature of SP1 and re-encrypts it using the session key with the DN before transmitting it to the DN. The DN descrambles the packet using the session key with the TSM and SP1 and verifies the integrity through the signature. After finishing the file transfer about the personal information, SP1 transmits the service provider information, forming a

partnership with the TSM, and it generates and transmits a unique ID notifying of the relationship between partnership and transmitted personal information file to the service provider and the NN. Metadata are updated by a block report of the DN, the file information received from the TSM and the ID-based NN.

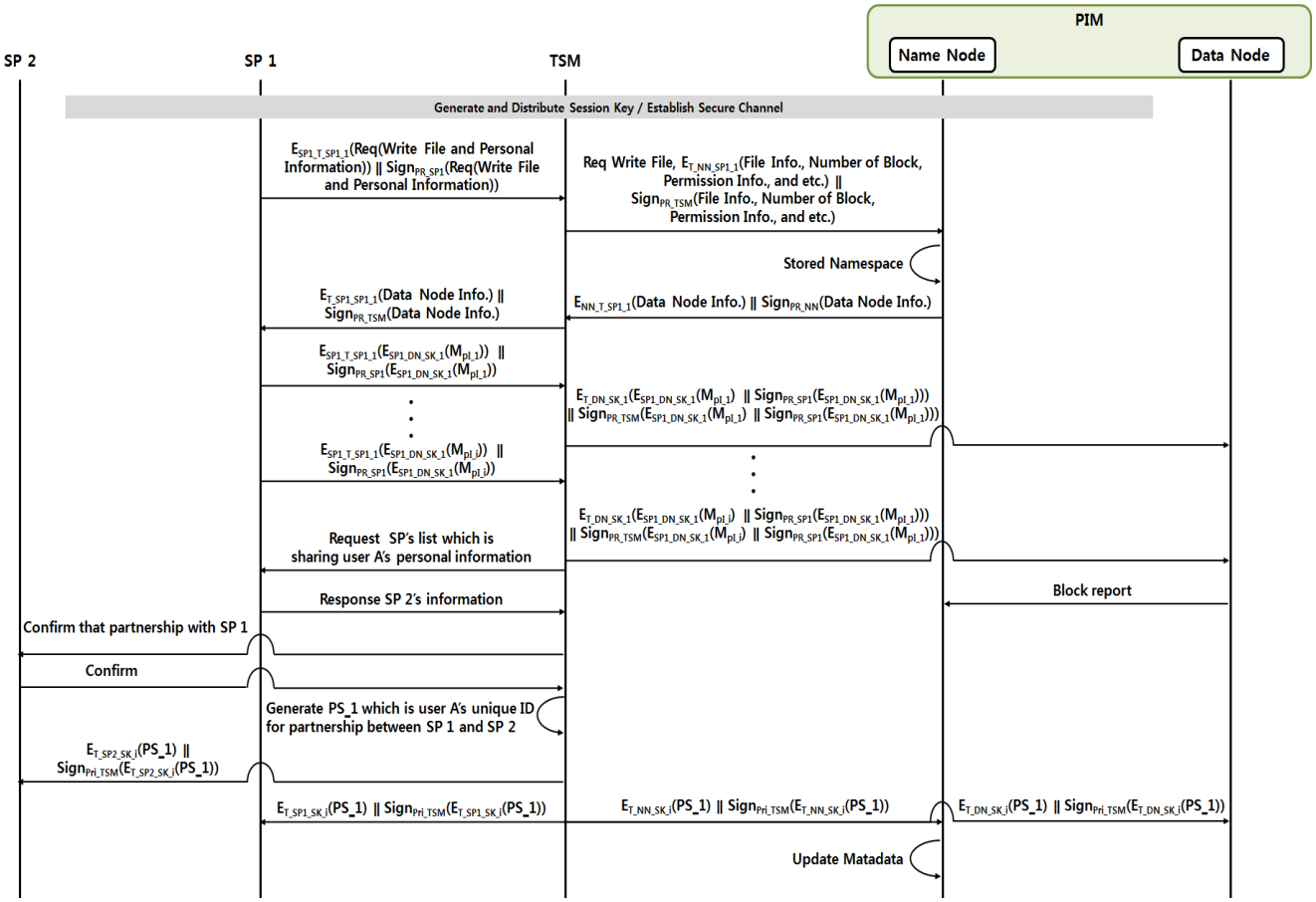

Figure 5. Personal information transmission protocol.

4.2.2. The Process of Accessing Pattern Information

Figure 6 shows the protocol of viewing the pattern information using the access key provided to the SP. The TSM, upon a request for viewing personal information or pattern information, uses a session key that was last used to verify Service Provider 2. To achieve this, instead of immediately transmitting a session key for session key security, the session key is hashed based on the random number generated by SP1 and the TSM in order to send the hashed session key for verification.

SP1 transmits a unique ID received during personal information file transfer to the TSM, and it transmits the applicable ID to the name node. The name node checks the metadata applicable to the ID-based personal information file, and the name node transmits the data node information to the TSM.

The TSM requests an access key matched with the ID to SP1, the NN and the DN, and each entity transmits the access key to the TSM. The TSM inserts the viewing authorization key that had been distributed into Formula (2) to restore and hash the secret value (PI_A_MK_TSM) and compares with the DN's stored hash value for verification. When the hash value verification at the TSM and PIM is successful, Service Provider 2 can view the personal information. The revision of personal information is operated

only when the authorization to view personal information and pattern information has been verified. The TSM inserts the restored secret value and the authorization key that had been distributed into Formula (1) to restore and hash the secret value and compare with the stored hash value for verification. When the verification of the hash value is successful at the TSM and the PIM is successful, Service Provider 1 can modify the personal information.

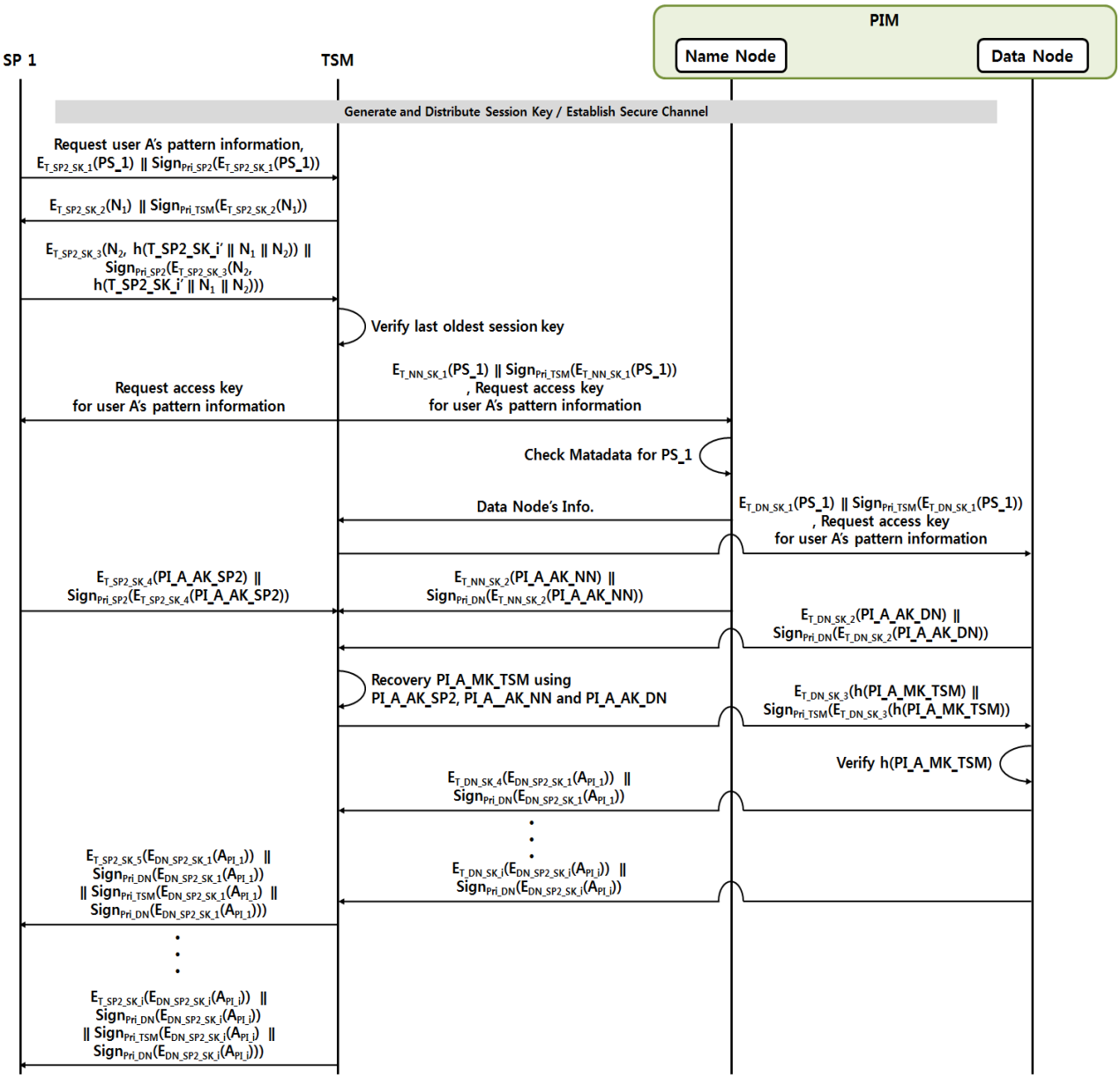

Figure 6. Pattern information transmission protocol.

5. Security and Performance Analysis

5.1. Security Analysis

Table 3 shows a comparative analysis of the suggested security schemes by various Hadoop security functions. It shows that the suggested scheme is secure to existing vulnerabilities of Hadoop [15,16,18]. One of the biggest problems in an existing Hadoop system is that access authority cannot be vested with

respect to the information, replay attack and key drain occurring between the name node and data node. Nonetheless, the protocol proposed provides secret sharing-based key generation and data protection between the name node and data node. Furthermore, by giving an access key to processing information consisting of general information, only information can be used that fits the authority given to the service providers.

Table 3. Comparative security analysis.

Check List	NoS_HDFS	RSA_HDFS	Ker_HDFS	HC_HDFS	Proposed Scheme
Authority management for information	Not support	Not support	Not support	Not support	Support
Leaked secret key	Vulnerability	Vulnerability	Vulnerability	Vulnerability	Secure
Replay attack	–	–	Vulnerability	Secure	Secure
Impersonation attack of the server	Vulnerability	Secure	Vulnerability	Vulnerability	Secure
Impersonation attack of the client	Vulnerability	Secure	Vulnerability	Vulnerability	Secure

5.1.1. Security Enhancement

To ensure that secure channels are formed during the communication between each domain, a public key between each domain is used to transmit secret information. The secret value is used to generate a session key. For secure communication when transmitting personal information, pattern information or information access keys, it was designed to be encrypted in two or three layers in the form of cipher-chaining. This also ensured that secret keys were used in the form of chaining or a secret sharing method was used, instead of processing the information using a shared secret key [19,20]. Lastly, when information is accessed, whether the user is a legitimate user is constantly verified. Simple accesses are prevented, and only through collaboration with other domains can the information be accessed [21–23].

5.1.2. Trusted System

Verification between each domain is made possible by using certification before transmitting practical information. When information or certification is provided between domains of different TSMs, the root TSM is used to form a trust-based system. Moreover, the trust of the information and system is ensured by having the process stages associated with the users' private information and the TSM shared, so that when information is provided, all domains related to the information have to provide a signature [24,25].

5.1.3. Efficient Cipher Key Used

A new key is not always generated in the protocol, but the key that had been used in the previous stage is used in the form of chaining when accessing or providing pattern information.

5.1.4. Non-Reputation

In the process stages that can be associated with the user's personal information, such as the storing of personal information, generation of pattern information, generation of an access key to pattern information

and access to pattern information, the transmitter's signature is required on the transmitted message to guarantee non-reputation. In addition, when cipher-chaining is used, not only the information transmitter, but also the domain that acts as a medium is required to offer its signature to enable non-reputation.

5.1.5. Replay Attack and Eavesdropping

When information is transmitted between service providers, the TSM and PIM, all data are encrypted by generating a session key and, therefore, are secure from eavesdropping. When the session key is generated, the seed value is constantly changed along with the secret shared value and random number to protect from replay attacks.

5.2. Performance Analysis

As can be seen in Table 4, the weight of the scheme has been made lighter than the existing security scheme for NFC integrated payment systems. Figure 7 shows that simply synchronizing the proposed security scheme is more effective than generating an authority key and distributing it within Hadoop. Figure 7 shows the secondary authentication key quantity resulting from increased data nodes when 10 service providers form one consortium. In implementing the authentication key using a block token in Hadoop, although the required key increases exponentially as the data nodes increase, the protocol set forth shows effective performance regardless of the secondary quantity of the data nodes, as the key increases depending on the relationship of the consortium.

Table 4. Comparative analysis with Kim's scheme.

Check List	Kim's Scheme [26]	Proposed Scheme
Number of stored keys for one user's personal information at the TSM	3 × (Number of relationships) + (Number of service providers)	(Number of relationships) + (Number of service providers)
Number of stored keys for one user's personal information at PIM	3 × (Number of relationships)	Number of relationships
Number of needed key for access of personal information	3 × (Number of service providers that are requesting personal information) + 2	2 × (Number of service providers that are requesting personal information) + 3

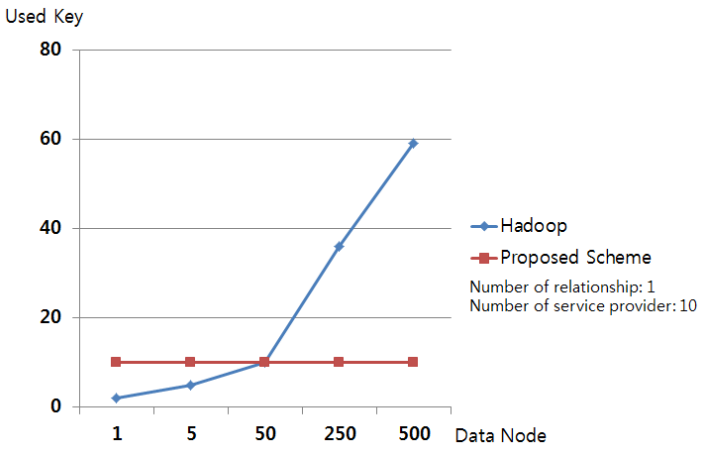

Figure 7. Number of used keys between Hadoop and the proposed scheme.

6. Conclusions

This paper suggested a communication security protocol based on the method of managing authority keys in order to ensure secure processing of the users' personal information. The suggested security scheme shows excellent security and performance compared to existing schemes. In addition, it has been designed with the NFC ecosystem in mind, allowing it to be applied to NFC integrated payment services. The paper has presented, for the first time in the field, a practical application of a context-rich system to an NFC integrated payment security system. As context-rich systems are emerging as the core of a future cyber world, this scheme is expected to be the start of many more applications to come. The main idea of the paper is distributing through a PIM-concentrated authority to the TSM and ensuring the anonymity and safety of pattern information and personal information. The distribution of the authority in that service may be impossible in case of problems with the TSM and PIM, so additional research is needed in this area.

Acknowledgments

This research was supported by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the ITRC (Information Technology Research Center) support program (NIPA-2014-H0301-14-4007) supervised by the NIPA (National IT Industry Promotion Agency).

Author Contributions

Jungho Kang researched relation work; Jungho Kang and Sangkee Suk designed the shceme; Jungho Kang and Jong Hyuk Park performed and analyzed the data; Jungho Kang and Sangkee Suk wrote the paper.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. Ibrahim, N.; Mohammad, M.; Alagar, V. Publishing and discovering context-dependent services. *Hum. Cent. Comput. Inf. Sci*. **2013**, *3*, doi:10.1186/2192-1962-3-1.
2. Soongsil University. *A Study on Privacy Protection Measure in NFC*; Korea Internet Security Agency: Seoul, Korea, 2011.
3. Kang, J. Design of Distributed Personal Information Management System for Secure Integrated Payment in NFC. Ph.D. Thesis, Soongsil University, Seoul, Korea, 2013.
4. Oh, J.S.; Park, C.U.; Lee, S.B. NFC-based mobile payment service adoption and diffusion. *J. Converg.* **2014**, *5*, 8–14.
5. Gnanaraj, J.W.K.; Ezra, K.; Rajsingh, E.B. Smart card based time efficient authentication scheme for global grid computing. *Hum. Cent. Comput. Inf. Sci*. **2013**, *3*, doi:10.1186/2192-1962-3-16.
6. Park, S.W.; Lee, I.Y. Anonymous Authentication Scheme based on NTRU for the Protection of Payment Information in NFC Mobile Environment. *J. Inf. Proc. Syst*. **2013**, *9*, 461–476.
7. GSM Association (GSMA). *Mobile NFC Technical Guidelines*, Version 2.0, 2007.

8. European Payments Council (EPC); GSM Association (GSMA). *Trusted Service Manager Service Management Requirements and Specifications*, Version 1.0, 2010.
9. Apache. Nutch and Hadoop Tutorial. Available online: http://wiki.apache.org/nutch/NutchHadoopTutorial (accessed on 28 May 2015).
10. Mike J. Cafarella Homepage. Available online: http://web.eecs.umich.edu/~michjc/bio.html (accessed on 28 May 2015).
11. Roy, I.; Setty, S.T.V.; Kilzer, A.; Shmatikov, V.; Witchel, E. Airavat: Security and Privacy for MapReduce. In Proceedings of the 7th USENIX Conference on Networked Systems Design and Mplementation, San Jose, CA, USA, 28–30 April 2010; pp. 1–20.
12. Park, S.H.; Jeong, I.R. A Study on Security Improvement in Hadoop Distributed File System Based on Kerberos. *J. Korea Inst. Inf. Secur. Cryptol*. **2013**, *23*, 803–813.
13. Lee, H. Use of big data hadoop platform. *Inf. Commun. Mag*. **2012**, *29*, 43–47.
14. Borthakur, D. The hadoop distributed file system: Architecture and design. Available online: http://hadoop.apache.org/docs/r1.0.4/hdfs_design.pdf (accessed on 28 May 2015).
15. Becherer, A. *Hadoop Security Design Just Add Kerberos? Really?* iSEC Partners, Inc.: San Francisco, CA, USA, 2010.
16. Seo, H. *Hadoop and Eco-System for Building of Big Data*; Week Technology Trends of National IT Industry Promotion Agency: Seoul, Korea, 2013; pp. 11–20.
17. O'Malley, O. Integrating Kerberos into Apache Hadoop. In Proceedings of the Kerberos Conference, Cambridge, MA, USA, 26–27 October 2010.
18. You, H. A Design of Group Key Management Systems for Secure Distributed File Systems in Big-Data Environment. Ph.D. Thesis, Soongsil University, Seoul, Korea, 2014.
19. Ogiela, M.R.; Ogiela, U. Linguistic Protocols for Secure Information Management and Sharing. *Comput. Math. Appl.* **2012**, *63*, 564–572.
20. Ogiela, M.R.; Sułkowski, P. Protocol for irreversible off-line transactions in anonymous electronic currency exchange. *Soft Comput.* **2014**, *18*, 2587–2594.
21. Degefa, F.B.; Won, D.H. Extended Key Management Scheme for Dynamic Group in Multi-cast Communication. *J. Converg.* **2014**, *4*, 7–13.
22. Chung, Y.S.; Choi, S.J.; Won, D.H. Lightweight anonymous authentication scheme with unlinkability in global mobility networks. *J. Converg.* **2013**, *4*, 23–29.
23. Vanus, J.; Kucera, P.; Martinek, R.; Koziorek, J. Development and testing of a visualization application software, implemented with wireless control system in smart home care. *Hum. Cent. Comput. Inf. Sci*. **2014**, *4*, doi:10.1186/s13673-014-0019-5.
24. Abbas, F.; Oh, H.K. A Step towards User Privacy while Using Location-Based Services. *J. Inf. Proc. Syst*. **2014**, *10*, 618–627.
25. Peng, K. A Secure Network for Mobile Wireless Service. *J. Inf. Proc. Syst*. **2013**, *9*, 247–258.
26. Kim, H.; Kang, J.; Jun, M. Study on Privacy Protection based on Secret Sharing in Near-Field Communication System. *IJACT Int. J. Adv. Comput. Technol.* **2013**, *5*, 486–496.