sustainability

MDPI

Article

Research on Digital Forensic Readiness Design in a Cloud Computing-Based Smart Work Environment

Sangho Park [1], Yanghoon Kim [2], Gwangmin Park [3], Onechul Na [1] and Hangbae Chang [4,*]

1 Department of Security Convergence, Chung-Ang University, Seoul 06974, Korea; sanghopark@cau.ac.kr (S.P.); nastop@cau.ac.kr (O.N.)
2 Department of Industrial Security, Far East University, Chungbuk 27601, Korea; yhkim@kdu.ac.kr
3 Forensics Center, Douzone ICT Group, Seoul 06193, Korea; gmpark@douzone.com
4 Department of Industrial Security, Chung-Ang University, Seoul 06974, Korea
* Correspondence: hbchang@cau.ac.kr; Tel.: +82-2-820-5538

Received: 29 December 2017; Accepted: 12 April 2018; Published: 16 April 2018

Abstract: Recently, the work environments of organizations have been in the process of transitioning into smart work environments by applying cloud computing technology in the existing work environment. The smart work environment has the characteristic of being able to access information assets inside the company from outside the company through cloud computing technology, share information without restrictions on location by using mobile terminals, and provide a work environment where work can be conducted effectively in various locations and mobile environments. Thus, in the cloud computing-based smart work environment, changes are occurring in terms of security risks, such as an increase in the leakage risk of an organization's information assets through mobile terminals which have a high risk of loss and theft and increase the hacking risk of wireless networks in mobile environments. According to these changes in security risk, the reactive digital forensic method, which investigates digital evidence after the occurrence of security incidents, appears to have a limit which has led to a rise in the necessity of proactive digital forensic approaches wherein security incidents can be addressed preemptively. Accordingly, in this research, we design a digital forensic readiness model at the level of preemptive prevention by considering changes in the cloud computing-based smart work environment. Firstly, we investigate previous research related to the cloud computing-based smart work environment and digital forensic readiness and analyze a total of 50 components of digital forensic readiness. In addition, through the analysis of the corresponding preceding research, we design seven detailed areas, namely, outside the organization environment, within the organization guideline, system information, terminal information, user information, usage information, and additional function. Then, we design a draft of the digital forensic readiness model in the cloud computing-based smart work environment by mapping the components of digital forensic readiness to each area. To verify the draft of the designed model, we create a survey targeting digital forensic field-related professionals, analyze their validity, and deduce a digital forensic readiness model of the cloud computing-based smart work environment consisting of seven detailed areas and 44 components. Finally, through an analytic hierarchy process analysis, we deduce the areas that should be emphasized compared to the existing work environment to heighten the forensic readiness in the cloud computing-based smart work environment. As a result, the weightings of the terminal information Universal Subscriber Identity Module(USIM) card, collect/gain virtual machine image, etc.), user information (user account information analysis, analysis of user's used service, etc.), and usage information (mobile OS artifact timeline analysis, action analysis through timeline, etc.) appear to be higher than those of the existing work environment. This is analyzed for each organization to preemptively prepare for the components of digital forensic readiness in the corresponding areas.

Keywords: future smart work environment; cloud computing; digital forensic; digital forensic readiness; digital evidence

1. Introduction

With the development of ICT technology, the work environment of organizations is changing. Existing ICT technology is utilized to produce, process, and store important information assets such as personal information, R&D information, and trade secrets in the divisions of the internal organization. As organizations expand, cooperation between divisions has become important, and ICT technology is utilized as a major system for cooperation within divisions such as Enterprise Resource Planning (ERP). ICT technology for simple data processing in a work environment within an existing organization has reached the level of offering a smart work environment where a cloud service is used to facilitate work cooperation between divisions and dynamically solve new problems. A smart work environment, based on a cloud environment where all data, information, and environments are sharable regardless of time and location, creates an environment where work can be conducted at any time and place; smart work environments include telecommuting, mobile working, and smart work centers. A work environment based on these cloud computing environments is expected to improve a corporation's productivity, enhance the effectiveness of the whole industry, and boost the industry competitiveness and added value of the whole corporation.

Environmental changes offer the advantage of being able to conduct work in the optimal period where work can be conducted, regardless of time and location, by active information sharing within the organization; however, it also increases the security risk of information sharing, in which important information within the organization can be utilized, processed, and saved externally through the network. Owing to these security risks of information sharing, leakage of information within organizations is increasing. The security risk owing to information sharing between the organization and the external environment caused limitations to existing borderline security systems that build sage environments by blocking internal contact points entering from outside the organization, such as anti-virus systems and network security systems. However, the majority of corporations initiate digital forensic investigations only after an incident occurs, without any experience and readiness of tools (equipment) regarding procedure and process, restoration of needed data, investigation, analysis, etc., to secure legal evidence in digital information. Accordingly, by processing indiscriminate digital forensic data and following an incorrect procedure and process, write protection for security incident equipment cannot be conducted in a timely manner or restored data may be unacceptable as legal evidence. In addition, there are increasing problems such as the vast range of doubt regarding the leakage incident time, users' wrong choices regarding the security incident, failure to acquire evidence owing to the data restore investigation, analysis targeting unrelated equipment, and an extended investigation period.

To solve this problem, the research requirement of digital forensic readiness is currently under discussion. Digital forensic readiness is defined as an organization's ability to minimize investigation cost and maximize the applicability of digital evidence [1]. Digital forensic readiness is a methodology that can analyze and level the current application ability for the process, tools, and technology of an organization's digital forensic investigation. Numerous organizations think of preparation for future security incidents as the lowest-priority task, or generate the results of introducing new digital forensic investigations after security incidents occur because they only consider it as political side of the inside and outside of the organization. Organizations that desire to prepare digital forensic readiness have difficulties in determining the kind of technical readiness required to gain digital forensic capability [2]. In particular, as explained earlier, with the development of ICT technology, organizations that pursue a change into a smart work environment equipped with immediacy need to ensure an appropriate level

of readiness with the investment of optimal resources, as it is difficult to invest identical manpower and expenses to the existing work environment.

In particular, unlike in the existing work environment, in cloud computing-based smart work environments, new security risks such as leakage of information assets from remote locations through the network occur owing to the reinforcement of information sharing. It is time to design a new digital forensic readiness considering environmental change.

Accordingly, in this research, we design a research method with digital forensic readiness at an optimum level by considering an organizational change from the existing work environment to a smart work environment. Specifically, we collect the organization's policy and technical readiness plan components by examining digital forensic readiness related literature. Then, we investigate and analyze whether these components satisfy the validity of appropriateness in constituting digital forensic readiness in the existing work environment or smart work environment. Finally, we analyze the digital forensic readiness area to be constituted preferentially in the individual work environment and clarify the differentiation of areas to be preferentially prepared in the existing work environment and smart work environment by comparing the areas. The smart work environment escapes the concept of the office, which is a designated work space based on cloud computing and is defined as a work environment in which work can be conveniently and effectively conducted regardless of location and time, such as in mobile environments. It is a system that utilizes not only an existing environment, but also work such as telecommuting, mobile work, and smart work centers.

2. Theoretical Background

2.1. Smart Work Environment Characteristics Based on Cloud Computing

Cloud computing is a type of internet-based computing, which is a technology that processes information with different computers connected to the internet, other than one's own computer. It provides shared computer processing resources and data to computers and other devices when requested. It is an environment where access is available regardless of location for configurable computing resources (e.g., computer networks, servers, storage, applications, services).

These cloud computing technologies can be classified as follows according to the materializing infrastructure [3].

- Private cloud—Environment technology materialized internally from a single organization;
- Community cloud—Dispersal environment technology composed of a group or business partner to share business resources;
- Public cloud—Shared environment technology that can be utilized by proving access to the public;
- Hybrid cloud—Technology utilizing more than two clouds.

The smart work environment built based on these clouds shows distinctive changes from the existing work environment, as shown in Table 1 [4].

Table 1. Changes in work environment according to the introduction of the cloud environment.

	Existing Work Environment	Smart Work Environment (Cloud)
User	Internal access based on PC or access through the internet	Combined wire-wireless access through multi-channel
Construct (Realization)	Individual construction by organization division (Realization)	Mutual utilization by organization division (Realization)
System	Wide variety of independent systems	Unity, standard, open-based system
Assets	Tangible asset (System)	Intangible asset (Service)
Ownership	Asset Ownership (Purchase)	Return/rent after usage (Mutual utilization)

The smart work environment escapes the concept of the office. It is a designated work space based on cloud computing and defined as a work environment in which work can be conveniently and effectively conducted regardless of time and location, such as in a mobile environment. It is a system that utilizes not only an existing environment but also work such as telecommuting, mobile work, and smart work centers (see Table 1).

In other words, the smart work environment is a working method with identical characteristics to those shown in Figure 1; there are no location and time constraints because mobile terminals such as smart phones and tablets are used, and users are able to conduct and process work immediately in both mobile situations or in the field. In other words, there is a rapid dispatch of various kinds of work, and the processing time of daily business such as approval and mail is reduced. In addition, this can increase work effectiveness by facilitating immediate communication and cooperation by becoming a flexible work environment. In other words, compared to existing work environments that are isolated within an organization or isolated, rigid work environments, the smart work environment can be referred to as an innovative work environment where flexibility and mobility exist [5]. These characteristics of the smart work environment have a lot of aspects in common with cloud computing, which enables an approach to computing resources placed in a remote place regardless of time and space, and increases the capacity for mutual cooperation between organization members, which leads to building a smart work environment based on cloud computing technology. In 2010, through the Telework Enhancement Act, the United States began operating a multiple smart work center using laptops, virtual private networks (VPN), etc. near Washington. In Korea, the smart work environment is being built rapidly by activities such as introducing smart work to public institutions where work should be conducted by widely moving within the region and enabling work to be conducted in smart work centers near one's house. Moreover, among European countries, The Netherlands is considered as the leader in smart work; according to the National Statistic Office of The Netherlands, in 2010, 59% of workplaces with more than ten people appear to be using smart work environments.

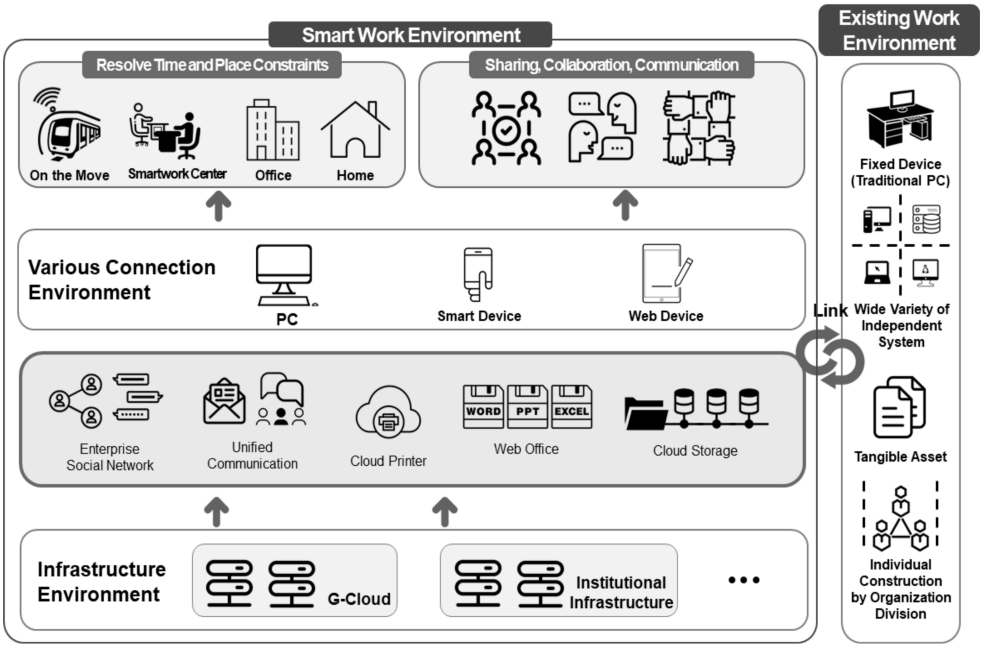

Figure 1. Future smart work environment characteristics based on the Cloud.

However, new security issues are arising owing to the development of new work environments. In corporations with existing traditional work environments, each individual uses a designated device (PC); however, in corporations using cloud computing-based smart work environments, official or

individual devices are used by several people. In addition, the complexity of work spaces increases from a fixed environment to multiple environments. Owing to these environmental characteristics, problems arise regarding important information leakage in organizations. First, a security issue exists in the terminals themselves, such as smart phones, tablets, and PCs. Theft and loss of these devices enables leakage of both personal and corporation information. According to Symantec, the risk of robbery and loss of smart phones is more than fifteen times higher than that of PCs. In addition to information leakage through these terminals, there is the risk of forgery of work information by accessing business servers illegally. Further, there are issues regarding networks and server security. Smart devices are used in a mobile environment rather than in a fixed environment, such as PCs, which can lead to the threat of hacking in the wireless section. In particular, in Wi-Fi and Bluetooth, sniffing (packet analyzer) and internet telephone wiretapping can occur through rogue Access Points (APs). Moreover, there are threats such as work data leakage and installation of malignant code (see Table 2).

Table 2. Changes in security issues according to work environment changes.

	Existing Work Environment	**Smart Work Environment (Cloud)**
Terminal Administration	Relatively low rate of terminal loss due to high usage rate of fixed terminal	Information leakage followed by diversity and loss of user terminals such as mobile terminal
Security Issue	Less danger of hacking in network section compared to smart work environment owing to high frequency of cable network usage utilizing a fixed terminal	Increase in hacking risk in wireless network section (Wi-Fi, Bluetooth, etc.) owing to high frequency of practical use in mobile environment using mobile terminals
Information Asset Ownership and Administration	Relatively low rate of information leakage danger by storing information assets internally, such as on servers within the organization	Occurrence of information leakage danger due to entrusting information asset storage to cloud service firms
Legislation and Regulations	Relatively easy to determine where the responsibility lies or conduct an audit when information leakage occurs	In the case of information leakage, matter of responsibility is ambiguous, and it is difficult to audit according to resource sharing

Security issues in these cloud computing environments generate various security incidents. Company A in the United States was saving clients' personal information in Company B's cloud server for operation of its back office (support task) and call center (support client). However, owing to a set-up error by the cloud service firm, outsiders were granted access to the corresponding cloud server, and client personal information leakage occurred. In a similar case, a cloud service provided by Company C lost 100,000 of the client company's websites owing to a zero-day attack of the virtualized platform (Hyper-VM) [6]. In these cases, security incidents such as information leakage did not occur within the victimized organization, and are instead referred to as occurrences of security incidents outside the organization due to improper maintenance by the cloud service operators used by the victimized corporations.

2.2. Digital Forensics Readiness

Nowadays, as corporations' work environments and data, such as documents, are being digitalized, the rate of digital evidence submitted in court lawsuits is gradually increasing. Thus, to prepare for court lawsuits, it has become important for corporations to maintain and preserve the admissibility of evidence for electronic documents or records that can potentially be evidence. According to these changes in the work environment, traditional information protection-centered incident investigations that do not follow strict rules of evidence have been limited in court

lawsuits, and digital forensic investigations that collect and preserve digital evidence equipped with admissibility of evidence for legal response have become important [7].

These digital forensic approaches can be classified into proactive forensics, active/live forensics, and reactive forensics according to the time of corresponding work performance. The majority of corporations utilize reactive forensics, which is considered to be a traditional forensic approach following the occurrence of a security incident, and only focus on forensic investigation of digital traces [8]. However, owing to the volatility and availability of forged digital evidence, if appropriate preparation of secure of digital evidence is not conducted beforehand, the digital evidence cannot be collected from the initial stages or can be damaged, which leads to the risk of not being able to secure admissibility of evidence, etc. Digital forensics that only focuses on reactive forensics has a limitation in terms of smooth incident investigation; to overcome this limitation, the need for a proactive forensic approach came to the fore [1].

Proactive forensics refers to the preparation for conducting forensics before digital forensic work is conducted following the occurrence of a security incident. The representative of proactive forensics is digital forensic readiness [9]. The definitions of various scholars regarding digital forensic readiness, when combined, conclude that digital forensic readiness must collect and analyze potential digital evidence in a state where it can provide legal evidence, and it must confirm the level of preparations in place beforehand. In addition, digital forensic readiness can also be described as having organizational preparedness beforehand to quickly secure potential legal evidence for security incidents that can occur as a result of various threats to the assets of the company, and having systemic, personnel preparations by having plans in place in advance [1].

For example, in the physical world, digital forensic readiness can be explained as realizing a physical security system that is executed to protect an organizations' assets, such as CCTV monitoring, security guard patrolling, and visitor record keeping in an online world [9]. The existing digital forensic framework predominantly comprises the content of the execution procedure using technology and specialized tools to conduct a digital forensic investigation [10]. However, digital forensic readiness is differentiated from the digital forensic framework as it is a preemptive and proactive counterstrategy that takes action at the systematic, organizational, and human level where evidence can be collected and analyzed effectively and rapidly before incidents occur [7].

Another characteristic of digital forensic readiness is, unlike existing information protection requirements, that digital evidence such as log history or monitoring results related to incidents are collected in the state of secured sincerity, integrity, completeness, reliability, etc., and secure legal admissibility of evidence. Accordingly, in the changing work environment, for corporations to conduct smooth incident investigations when infringement incidents occur, they should be freed from existing restore-centered information protection-based incident responses and reactive forensic-centered incident counterstrategies; instead, they need to establish an incident counterstrategy that can complexly perform proactive, reactive forensic investigations by establishing digital forensic readiness.

In particular, in the cloud computing-based smart work environment, there are many cases where digital evidence in server systems of remote areas is collected separately from the local system, which can be a complicated process that requires considerable time for the collection of digital evidence and makes it difficult for the company to collect digital evidence after it realizes that a security incident has occurred [11]. Thus, a preemptive audit (analysis) through digital forensic readiness is required to conduct fast, efficient digital evidence collection and analysis at the corporate level.

Since the concept of digital forensic readiness was first proposed, in order to establish digital forensic readiness suitable for each corporation's characteristics and environmental characteristics, a digital forensic readiness model with organized components such as logging technology, logging target, security of evidence technology, handling evidence, etc. is being examined by numerous researchers.

In research reported by Sachowski [12], it was concluded that in order to effectively materialize digital forensic readiness programs within corporations, maximize the ability of collecting digital evidence, and minimize the cost of digital forensic investigations for the occurrence of security

incidents, certain aspects of digital forensic readiness should be included in the requirements of information security: defining the business risk scenarios that require digital evidence, identifying available data sources and different types of digital evidence, etc. Beyond this, the report stated that determining the requirements for gathering digital evidence and establishing capabilities for gathering digital evidence in support of evidence rules should be included in the requirements of information security. It suggested a basic approach in order to effectively materialize digital forensic readiness programs within corporations by designing and developing targeted security monitoring controls to detect events.

Endicott et al. [13] proposed a checklist that can identify an organization's digital forensic readiness and technical requirements that can safely save and process digital forensic evidence; this checklist is proposed as digital forensic readiness model components. Rafique et al. [14] proposed log administration technology, hashing technology, data search technology, data collection and normalization technology, etc. to effectively collect and analyze digital evidence while maintaining the legal admissibility of the evidence as components of a digital forensic readiness model. In addition, Kim et al. [15] proposed penetration testing and data collection technology as components of the digital forensic readiness model. Hale [16] proposed an effective electronic record administration system and dispersion monitoring technology as components of the digital forensic readiness model. In addition, Al-Mahrouqi et al. [17] and Kebande & Venter [18] proposed a technical requirement for the digital forensic readiness model while suggesting profiling technology, network design technology, computer and server technology, etc. as components for the digital forensic readiness model for effective digital forensic investigation.

However, to effectively collect and analyze digital evidence, various policy requirements are needed in addition to the technical requirements, and numerous recent studies have been conducted to deduce these. Elyas et al. [9] proposed the following components of the digital forensic readiness model: legal requirements and contents regarding organization members' regular education and training, awareness enhancement activity, digital forensic and monitoring policy, etc. to smoothly conduct digital forensic investigations. Reddy & Venter [19] proposed the following components of the digital forensic model: deploying exclusive personnel for digital forensic applies incident investigation, procedure preparation of incident investigation, procedure preparation for preservation of digital evidence, digital forensic education training for organization members, and enhancing awareness training. In addition, Kohn et al. [20] proposed the following components of the digital forensic readiness model: evidence collection and preservation policy, information system usage policy, etc. Through the studies of Elyas et al. [2] and Kim et al. [15], the organization's culture regarding digital forensic investigation, governance structure, etc. was proposed as a component of the digital forensic readiness model; in addition, they proposed policy requirements needed for digital forensic readiness.

These introductions to and operation of digital forensic readiness can increase the cost efficiency by shortening the process of the digital forensic investigation when incidents occur and suppressing insiders' potential mental state of information leakage by facilitating the tracing of the cause and responsibility of an incident, which enhances the corporation's overall security level. Further, by showing that corporations are enacting reasonable protection of and response action for their information assets, they can increase their information credibility and the likelihood of winning a case and exemption in lawsuit [9].

3. Designing a Digital Forensic Readiness Model in a Cloud Computing Environment

3.1. Research Methodology Design

To design a digital forensic readiness model in a cloud computing-based smart work environment, we analyzed research methodologies by examining precedent research [1,2,9] for the design of digital forensic readiness models for the existing work environment. In addition, we designed a

research methodology where relevant contents are added to reflect the characteristics of the cloud computing-based smart work environment (see Figure 2).

First, in order to reflect the altered environmental characteristics, we have elucidated a difference from existing work environments by investigating research in the literature on digital forensic readiness. In addition, using digital forensic readiness-related research reports, we have conducted a comparison of both concepts and differences between proactive digital forensic investigations, which preemptively respond to security incidents, and reactive digital forensic investigations, which were mostly about existing information security incidents. Furthermore, we conducted a comparison of concepts and differences between digital forensic investigation and digital forensic readiness and analyzed the various components which comprise a digital forensic readiness model. Second, we have designed composition areas for classifying components of a digital forensic readiness model which was investigated in preceding research, and designed a draft of a digital forensic readiness model in cloud computing-based smart work environments by connecting the appropriate components of digital forensic readiness models.

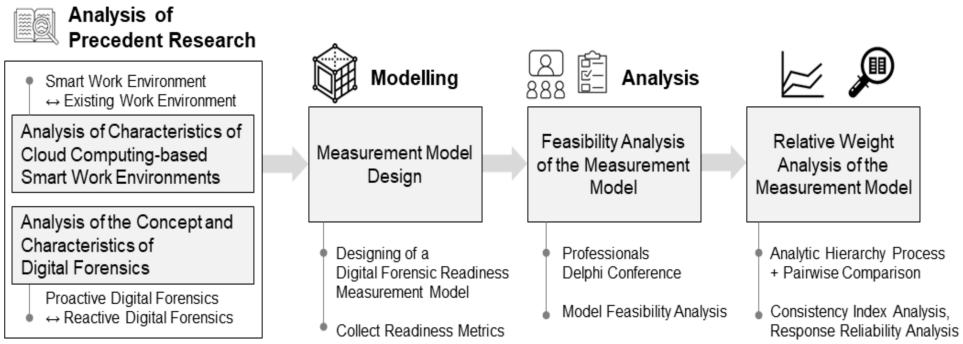

Figure 2. Digital forensic readiness design research model.

We created a survey targeting 30 digital forensic-related experts to analyze the validity of each component of our draft design for a digital forensic readiness model. Using the results of this survey, components that were found to be insufficient in validity were removed. Lastly, we have conducted an additional survey in order to determine which areas should be relatively emphasized compared to existing work environments, to enhance the forensic readiness in cloud computing-based smart work environments. We conducted an analytic hierarchy process analysis, targeting a reselected 15 out of 30 digital forensic-related experts who had carried out the validity analysis.

3.2. Designing a Readiness Model for Digital Forensic Readiness Measurement in the Cloud Computing-Based Smart Work Environment

By combining the definitions and processes of digital forensic readiness in precedent research, digital forensic readiness models can be categorized into nontechnical policy requirements and technical requirements. Policy requirements can be categorized further into requirements within the organization and requirements outside of the organization. To secure the ability to act as digital evidence, the reliability of the digital forensics analyst and tools must be guaranteed. Moreover, as it requires documented procedures, basically the component elements of the digital forensics expert/tools and technology/procedures that can be trusted must be included.

The results of the analysis of the digital forensic readiness model show that the importance of policy requirements has been increasing recently, and the trend is changing from existing simple procedure models to comprehensive structure models. That is, in addition to preparing a technology infrastructure related to digital forensics within the organization, it is evolving into a form of digital governance that covers technical/nontechnical requests within/outside the organization.

In addition, the trend is to establish digital forensic readiness strategies based on legislation related to international standards, rather than digital forensic readiness strategies centered on the company. From the perspective of company-wide risk management, digital forensic readiness is demanded as an integrated model that covers tools, personnel, and policies for the collection and preservation of evidence that can be used in court.

Existing digital forensic readiness models are reactive response readiness models based on general security incidents. Digital forensics readiness that handles post-security-incident measures cannot be applied to security incidents in a cloud computing environment [21,22]. Such an environment requires proactive ability, and thus a digital forensic readiness model needs to be presented in consideration of the characteristics of cloud computing-based smart work environments.

Therefore, to design a readiness model to measure digital forensic readiness in a cloud environment, we designed separators and collected elements from precedent research, and these are mapped in Tables 3 and 4.

In this research, we created digital forensic readiness based on the analyzed research of existing digital forensic readiness models. First, to distinguish the areas of digital forensic readiness modeling, we accommodated the existing classification of precedent researches mentioned in Tables 3 and 4 and largely divided these into non-technical policy readiness and technical readiness. In addition, the areas of policy readiness were distinguished by segmenting them into "outside the organization environment" and "within the organization guideline", as classified in the existing precedent research [2–31]. However, in the precedent research, the classification of detailed areas for the design of a specific digital forensic readiness model was limited since segmented areas for technical readiness were not distinguished. Accordingly, in this research, we have distinguished detailed areas of technical readiness, namely system information, terminal information, user information, usage information, additional function, etc., by inspecting precedent researches of system models used in cloud computing-based smart work environments, as well as digital forensic framework related precedent research. Component areas of the digital forensic readiness model, which were organized through the analysis of preceding research, were rearranged to follow the order of work flow required for the introduction of digital forensic readiness and were applied to the digital forensic readiness model (see Figure 3).

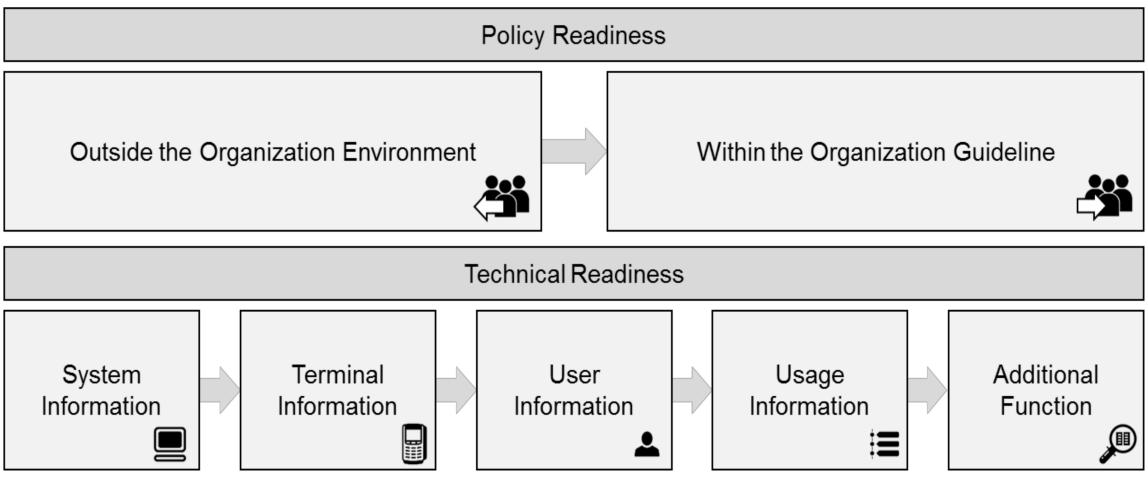

Figure 3. Design of a detailed area of the digital forensic readiness model.

Table 3. Analysis of components for designing a digital forensic readiness model in a cloud computing-based smart work environment (policy requirement).

Component	[2]	[9]	[13]	[15]	[19]	[20]	[23]	[24]	[25]	[26]
(1) Adhering to legal requirements		●								●
(2) Legal requirements	●	●								
(3) Interacting with law enforcement organizations	●	●			●					
(4) Case report guide for investigation institutions					●					
(5) Information sharing and cooperation with external organizations					●					
(6) Establish single contact point with law enforcement organizations					●					
(7) Education and training targeting employees, and regular reminder activities	●	●			●					
(8) Digital forensic education and training, and awareness improvement activities	●	●			●					
(9) Internal/External training	●	●			●					
(10) Internal digital forensic ability maintenance or external professional identification and usage policy		●								
(11) Policy content education and training targeting employees	●	●			●					
(12) Create an exclusive forensics department		●								
(13) Incident response personnel establishment					●					
(14) Forensic policy	●	●			●					
(15) Monitoring policy	●	●		●		●			●	
(16) Comprehensive digital forensic management framework	●	●								
(17) Forensic readiness policy				●		●				
(18) Forensic incident response roles and responsibilities policy					●	●				
(19) Establish evidence preservation policy								●		
(20) Forensic readiness procedure				●	●	●				
(21) Forensic investigation procedure				●	●	●				
(22) Check lists			●							
(23) Organizational culture	●	●								
(24) Governance structure	●	●								
(25) Prepare forensics solutions							●			

Table 4. Analysis of components for designing a digital forensic readiness model in a cloud computing-based smart work environment (technical requirements).

Component	[8]	[14]	[15]	[16]	[17]	[18]	[19]	[22]	[23]	[24]	[27]	[28]	[29]	[30]	[31]
(26) Forensic evidence processing			●		●	●	●			●					
(27) Forensic equipment and tools									●		●				
(28) Composer metadata	●														
(29) Usage time record		●											●		●
(30) Search support technologies		●													
(31) Log management technologies		●		●	●							●	●	●	
(32) Kernel/file system access tracking		●		●									●		●
(33) Hashing technologies		●													
(34) Data collection and normalization		●													
(35) Integrity-securing algorism application		●											●		
(36) Infrastructure preparation									●						
(37) Encryption of files and communication channels			●												
(38) Safe storage technologies			●	●			●							●	
(39) Model intrusion test			●												
(40) Attacker estimation graph					●										
(41) Profiling technologies					●										
(42) Network design						●									
(43) Computer and Server technologies						●									
(44) Intrusion detection system							●								
(45) Integrity verification technologies								●							
(46) Distribution monitoring data sharing and link technologies				●										●	

When conducting digital forensics in a cloud computing-based smart work environment, user information regarding which users have actually used an official device shared by several users should be traceable. Moreover, digital forensics should be conducted consuming minimal time and cost in collecting digital evidence in order to minimize business disruption [32].

However, there is a limit to reflecting all the characteristics required to perform digital forensics in a cloud computing-based smart work environment with only the precedent research arranged in Tables 3 and 4. To solve this problem, we referred to research regarding digital forensics in cloud computing environments [33–35] and determined the additional major components required to conduct digital forensics in a cloud computing-based smart work environment. We designed a digital forensic readiness model in a cloud computing-based smart work environment by connecting the components of the final and seven previously designed detailed areas (outside the organization environment, within the organization guideline, system information, terminal information, user information, usage information, and additional function). In this model, the components are designed to form a digital forensic readiness model that can cope with business processes, risk scenarios, and internal information leakage regarding the cloud computing-based smart work environment. Components are also designed to satisfy requirements such as integrity, reliability to ensure legal admissibility of evidence by reflecting internal business requirements, and legal requirement from outside of the organization.

In particular, technical requirements were constructed to prevent advanced leakage of internal information by focusing on the analysis of the action of leaking (people-based). Acts of copying and extracting data from laptops or PCs using external hard drives or flash drives are determined through the analysis of traces of access and data transfer using flash drives and external hard drives (registry and Windows system log analysis, link file analysis, shortcut files to recently opened documents, etc.). Acts of transferring classified documents using e-mail are determined through the analysis of traces of e-mail sending and their attachments—Outlook data file (PST, OST) analysis and restoration analysis of other mail database files. Traces of the use of data deletion tools and deliberate acts of damage are determined through the analysis of traces of using data deletion tools and analysis of deleted data—registry and free patch (traces of activation of executable programs), and restoration of deleted data through data carving. Acts of forging/changing and copying of data, such as classified documents, floor plans, and other plans, are determined by identification by the creator of the original document (document metadata analysis, file integrity analysis using hash functions, and file similarity verification using fuzzy hash). Acts of information leakage using Web hard drives and by accessing other websites are determined through website access breakdown analysis and analysis of traces of shared network access—analysis of usage traces of Web browsers (temporary internet folder analysis), and network-related registry analysis. Finally, to confirm the user of the related media and OS installation information, the OS installation information and timeline is confirmed—analysis of user usage patterns (circumstances) using time series analysis and installation information analysis using OS artifact analysis (see Table 5).

Table 5. Digital forensic readiness model for a cloud computing-based smart work environment (draft).

Area (Reference Mapping)		Component and Description
Policy readiness	Outside the organization environment (1), (2), (3), (4), (6)	-Adhere to digital forensics related standards/guidelines: Secure integrity/reliability of digital evidence by adhering to digital forensics related standards/guidelines -Adhere to legal requirements: Adhere to legal procedure (secure suitability/objectivity) -Establish single contact point with law enforcement organizations: Establish single contact point with law enforcement organizations for continuous interactions regarding court cases -Produce incident report guideline for investigative agency: Guide production to organize processes and methods in order to report to the investigative agency when incidents occur
	Within the organization guideline (7), (8), (9), (11), (12), (13), (14), (15), (16), (17), (18), (19), (20), (21), (25)	-Prepare forensics solutions (proactive/detailed analysis tools): Secure a proactive evidence collection system through preparation of forensics solution -Prepare forensics equipment (writing prevention devices, copiers, etc.): Secure proactive evidence collection system through preparation of forensics equipment -Identify and categorize information assets: Identify and categorize information assets for effective administration thereof -Assign responsibility of information assets: Assign responsibility of information assets to reinforce responsibility traceability when information assets infringement incidents occur -Secure confidentiality agreements, etc.: Secure confidentiality agreements, etc. to reinforce organization members' security consciousness and responsibility -Establish an evidence preservation system (server): Maintain safe preservation and integrity of original evidence through the construction of an evidence preservation system (server) -Use proven forensics tools: Secure the reliability/objectivity of forensic tools -Create an exclusive forensics department (personnel): Create an exclusive department (personnel) to conduct an effective digital forensic -Educate and train employees considering environmental changes: Educate and train employees periodically to cope with the rapidly changing environment -Establish evidence preservation policy: Maintain safe preservation and integrity of original evidence through the development of an evidence preservation policy -Establish personnel audit policy: Ensure legitimacy of internal audit
Technical readiness	System information (31), (32), (34), (42)	-Analyze the basic system information: Analyze the system environment by analyzing basic system information -Analyze system on/off time: Analyze the system environment by analyzing the system on/off time -Examine the system access authority: Analyze the system environment by examining the system access authority -Analyze the installed program breakdown: Analyze the system environment by analyzing the installed program breakdown -Analyze the auto-execution program breakdown: Analyze the system environment by analyzing the auto-execution program list -Analyze the network information: Analyze the network environment such as IP/MAC Address and bandwidth -Analyze the shared folder breakdown: Analyze the network environment such as shared folder breakdown -Analyze the external storage memory connection breakdown: Analyze the user's act of usage to confirm if external storage memory should be used -Analyze the anti-forensic trace: Analyze the user's act of usage to confirm if anti-forensic analysis should be conducted -Analyze the virtualization environment construction trace: Analyze the user's act of usage to confirm if the virtualization environment should be constructed -Analyze the cloud service synchronization breakdown: Analyze the user's act of usage to confirm if the cloud service should be utilized
	Terminal information (38)	-Secure volatility memory within the terminal: Secure volatility data that can easily disappear in the terminal -Collect/gain flash memory: Flash memory data gain for terminal analysis -Collect/gain microSD cards: Gain microSD cards data for terminal analysis -Collect/gain USIM cards: Gain USIM cards for terminal analysis -Collect/gain virtual machine image: Collect/gain virtual machine image for virtualization environment analysis in the case of virtualization environment-built terminals
	User Information (41)	-Analyze user account information: Analyze basic information on user account -Analyze user registry: Analyze basic information on user account -Analyze visited website information: Analyze the user's website usage pattern -Analyze portal search words: Analyze the user's website usage pattern -Analyze recently opened documents: Analyze the user's document data (local system) act of use -Analyze recently executed programs: Analyze the user's application program act of use -Analyze executed commands: Analyze the user's command act of usage -Analyze the user's used services: Analyze the user's service act of use
	Usage Information (29), (40)	-Analyze window artifact timeline analysis: Analyze mainly used OS artifact timeline in fixed terminal -Analyze Mobile OS (Android/iOS, etc.) artifact timeline: Analyze OS artifact timeline of primary mobile terminal -Analyze MAC file timeline: Analyze the user's file usage pattern according to flow of time -Analyze action through timeline: Analyze the user's action according to flow of time -Apply credible time stamp: Apply credible time stamp to clearly confirm flow of time
	Additional Function (30), (33)	-Provide prompt file searches: Provide file searches for prompt digital forensic performance -Search and analyze large files: Provide large file searches to analyze cloud computing servers retaining large files -Analyze the existence of unauthorized files: Provide searches to confirm if files are authorized -Search encrypted files and decrypt: Provide searches for encrypted file analysis -Analyze of hidden files by changing the extension: Provide searches for hidden files analysis -Derive hash values for searched files: Derive hash values to enhance search reliability -Search files including personal information: Provide file searches containing sensitive personal information

3.3. Verification of Digital Forensic Readiness Model in Cloud Computing-Based Smart Work Environment

To evaluate the validity and weighting of the digital forensic readiness model in the cloud computing-based smart environment derived from the analysis of related literature regarding digital

forensic readiness and analysis of the characteristics of cloud computing environments, we collected survey data from 30 professionals with more than three years of practical experience related to digital forensics.

We gathered survey data targeting 30 experts with more than three years of field experience regarding digital forensics. Targeted experts were gathered using a snowball sampling method, which gradually increases the number of people by obtaining recommendations of other experts related to this field by the initial survey participants. The initial survey participants targeted three experts who worked for more than three years in a digital forensic division of a company that offers professional ICT solutions and information, communication services, and has a digital forensic related certificate. Henceforth, through the introduction of corresponding experts, we carried out the survey targeting experts who have worked in the digital forensic field for more than three years, acquiring a digital forensic related certificate, or have legal experience related to digital evidence. Finally, 30 experts were gathered from five digital forensic related corporations (or divisions) and two from a law firm specializing in ICT. Half of the digital forensic experts have a digital forensic related certificate; 8 out of 30 have legal experience regarding digital evidence, and 7 out of 30 have both a digital forensic related certificate and legal experience regarding digital evidence.

For the validity survey of the digital forensic readiness model in a cloud computing-based smart environment, the evaluation criteria of the questionnaire were constructed based on the seven areas of the derived model (outside the organization environment, within the organization guideline, system information, terminal information, user information, usage information, and additional function). We had them evaluate the seven areas using a Likert five-point scale, and we included the criteria of existing work environment and smart work environment and had them evaluate the validity for each criterion so as to compare objectively whether the proposed model is appropriate to cloud computing-based smart environments.

To examine the reliability of each preferentially retrieved questionnaire result, we calculated Cronbach's α through the following equation.

$$\mathrm{a} = \frac{K}{K-1}\left(1 - \frac{\sum_{i=1}^{k} {\sigma^2}_{Y_i}}{{\sigma^2}_X}\right)$$

where K: number of questions, ${\sigma^2}_{Y_i}$: i-th score of question dispersion, and ${\sigma^2}_X$: total score dispersion.

Cronbach's α for the existing work environment questionnaire was calculated as 0.972, Cronbach's α for the smart work environment questionnaire was calculated as 0.951. Generally, it is deemed to be reliable if Cronbach's α is over 0.7 [36]. Analysis of the results show that the validity of the digital forensic readiness components in the existing work environment and smart work environment are both reliable.

In this research, the Likert five-point scale was used to determine the validity of each component. In the Likert five-point scale, values below 3.5 are regarded as an average [37]. Accordingly, components that are below 3.5 are determined to have a relatively lower importance in the cloud computing-based smart work environment, which leads to elimination in the designed digital forensic readiness model.

High values were calculated for both "outside the organization environment" and "within the organization guideline" in the existing work environment (3.90 and 3.87, respectively) and the smart work environment (4.04 and 3.95, respectively).

In the system information and additional function areas, the validity of the existing work environment (3.79 and 3.90, respectively) was higher than that of the smart work environment (3.63 and 3.63, respectively). In the user information area, the values for usage information area, terminal information area, and smart work environment (3.87, 3.68, and 3.83, respectively) were higher than those for the existing work environment (3.67, 3.53, and 3.68, respectively). The values for all seven composition areas were above 3.5, which satisfies the validity of all composition areas. However, as we verified in the specific component elements unit, the results showed that the value of

the production of incident report guidelines for an investigative agency from outside the organization area, assigning responsibility by information assets from within the organization area, system access authority examination from system information area, secure volatility memory within the terminal from terminal information area, user registry analysis from user information area, and file searches including personal information from the information identification area, were all less than 3.5 for both the existing work environment and the smart work environment, which does not satisfy the validity. In addition, the value for the mobile OS artifact timeline analysis from the usage information within the existing work environment and the value for the window artifact timeline analysis from the usage information within the smart work environment were less than 3.5, which also does not satisfy the validity (see Table 6).

Table 6. Validity analysis result of digital forensic readiness components in the smart work environment.

Area (Reference Mapping)		Component	Validity	Acceptance
Policy readiness	Outside the organization environment (1), (2), (3), (4), (6)	Adhere to digital forensics related standards/guidelines	4.37	O
		Adhere to legal requirements	4.27	O
		Establish single contact point with law enforcement organizations	4.33	O
		Production of incident report guideline for investigative agency	3.20	X
		Average Validity Outside the Organization Environment	**4.04**	
	Within the organization guideline (7), (8), (9), (11), (12), (13), (14), (15), (16), (17), (18), (19), (20), (21), (25)	Prepare forensics solutions (proactive/detailed analysis tools)	3.97	O
		Prepare forensics equipment (writing prevention devices, copiers, etc.)	3.97	O
		Identify and categorize information assets	4.00	O
		Assigning responsibility by information assets	2.87	X
		Secure confidentiality agreements, etc.	4.10	O
		Establish evidence preservation system (server)	4.03	O
		Use proven forensics tools	4.17	O
		Create an exclusive forensics department (personnel)	4.13	O
		Employee education and training considering environmental changes	4.03	O
		Establish evidence preservation policy	4.20	O
		Establish personnel audit policy	4.00	O
		Average Validity within the Organization Guideline	**3.95**	
Technical readiness	System information (31), (32), (34), (42)	Analyze basic system information	3.80	O
		Analyze system on/off time	4.13	O
		System access authority examination	2.73	X
		Analyze installed program breakdown	3.80	O
		Analyze auto-execution program breakdown	3.60	O
		Analyze network information	3.47	O
		Analyze shared folder breakdown	3.67	O
		Analyze external storage memory connection breakdown	3.63	O
		Analyze anti-forensic trace	3.97	O
		Analyze virtualization environment construction trace	3.93	O
		Analyze cloud service synchronization breakdown	3.73	O
		Average Validity of System Information	**3.68**	
	Terminal information (38)	Secure volatility memory within the terminal	3.07	X
		Collect/gain flash memory	4.17	O
		Collect/gain microSD cards	4.03	O
		Collect/gain USIM cards	3.90	O
		Collect/gain virtual machine image	3.97	O
		Average Validity of Terminal Information	**3.83**	
	User Information (41)	Analyze user account information	4.07	O
		User registry analysis	3.27	X
		Analyze visited website information	4.03	O
		Analyze portal search word	3.90	O
		Analyze recently opened documents	3.93	O
		Analyze recently executed programs	3.97	O
		Analyze executed commands	3.90	O
		Analyze user's used services	3.90	O
		Average Validity of User Information	**3.87**	
	Usage Information (29), (40)	Window artifact timeline analysis	2.63	X
		Analyze mobile OS (Android/iOS, etc.) artifact timeline	3.93	O
		Analyze file MAC timeline	4.10	O
		Analyze action through timeline	4.13	O
		Apply credible time stamp	3.60	O
		Average Validity of Usage Information	**3.68**	
	Additional Function (30), (33)	Provide prompt file search	3.77	O
		Analyze large file searches	3.53	O
		Analyze existence of unauthorized files	3.90	O
		Search for encrypted files and decrypt	3.70	O
		Analyze hidden files by changing the extension	3.93	O
		Derive hash values for searched files	3.73	O
		File searches including personal information	2.83	X
		Average Validity of Additional Functions	**3.63**	

Note: Major summary part are marked in style "bold".

The reason for these differences in the component validity verification processes of the existing work environment and smart work environment seems to be attributed to the type of terminal used in each environment and the fact that the OS mounted on the terminal is differs between environments.

Additionally, to determine the forensic readiness in a cloud computing environment that needs to be established first based on each environment, we conducted an analysis of the relative priority for each subordinate area; that is, we conducted an analytic hierarchy process to calculate the weightings.

To perform the analytic hierarchy process analysis, we developed a questionnaire consisting of a combination of detailed sections to allow the relative importance between detailed sections to be surveyed. In the analytic hierarchy process analysis, the selection of a group of experts in certain corresponding fields and the truthfulness and consistency with which the respondents answered the survey is considered to be more important than focusing on sample size [38]. Therefore, of the 30 digital forensic experts who participated in the validity analysis survey, we reselected 15 experts with more than seven years of experience; then, we distributed the questionnaire and analyzed the results. To examine the consistency of the judgement of the results of each retrieved questionnaire, a consistency index was calculated. Generally, if the consistency index is less than 0.1, it is deemed to be reliable and consistent. The consistency index for each work environment was 0.075 for the existing work environment, and 0.086 for the smart work environment, which was considered to be consistent.

We used mathematical methods on the pairwise comparison matrix to calculate the relative importance and relative preference for the decision-making factors in each class (see Figure 4). In further detail, we calculated $\lambda_{max,}$ which is the largest λ (lambda) that satisfies the following equation, and its corresponding ω (vector).

$$A \cdot w = \begin{bmatrix} \frac{w_1}{w_1} & \frac{w_1}{w_2} & \frac{w_1}{w_3} & \cdots & \frac{w_1}{w_n} \\ \frac{w_2}{w_1} & \frac{w_2}{w_2} & \frac{w_2}{w_3} & \cdots & \frac{w_2}{w_n} \\ \frac{w_3}{w_1} & \frac{w_3}{w_2} & \frac{w_3}{w_3} & \cdots & \frac{w_3}{w_n} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ \frac{w_n}{w_1} & \frac{w_n}{w_2} & \frac{w_n}{w_3} & \cdots & \frac{w_n}{w_n} \end{bmatrix} \cdot \begin{bmatrix} w_1 \\ w_2 \\ w_3 \\ \vdots \\ w_n \end{bmatrix} = \begin{bmatrix} nw_1 \\ nw_2 \\ nw_3 \\ \vdots \\ nw_n \end{bmatrix} = n \begin{bmatrix} w_1 \\ w_2 \\ w_3 \\ \vdots \\ w_n \end{bmatrix}$$

$$A \times \omega = \lambda_{max} \times \omega,$$

Figure 4. Pairwise comparison matrix.

As a result, we can calculate the relative importance of each work environment, as shown in Tables 7 and 8.

Table 7. Pairwise comparison matrix values between measured factors in an existing work environment.

Existing Work Environment	Outside the Organization Environment	Within the Organization Guideline	System Information	Terminal Information	User Information	Usage Information	Additional Function
Outside the organization environment	1	3.70	3.79	3.89	3.89	3.97	3.48
Within the organization guideline		1	3.01	3.21	2.71	3.28	3.13
System information			1	2.82	2.02	2.21	2.32
Terminal information				1	2.29	1.52	0.65
User information					1	3.01	2.33
Usage information						1	1.29
Additional function							1

Table 8. Pairwise comparison matrix values between measured factors in a smart work environment.

Smart Work Environment	Outside the Organization Environment	Within the Organization Guideline	System Information	Terminal Information	User Information	Usage Information	Additional Function
Outside the organization environment	1	2.94	3.07	2.58	3.89	3.01	3.32
Within the organization guideline		1	2.86	2.96	3.24	3.48	3.48
System information			1	0.68	0.60	2.12	2.45
Terminal information				1	1.63	1.42	0.51
User information					1	2.40	2.11
Usage information						1	3.36
Additional function							1

Note: Symmetric part where identical data is being overlapped in pairwise comparison matrix data is omitted and marked in style "shade".

The deduced weight for the existing work environment and smart work environment is identical to the values shown in Table 9. First, the areas outside the organization environment and within the organization guideline had the highest percentage in the existing work environment and smart work environment. This indicates that the policy readiness area is crucial in two environments. In the smart work environment, three areas, namely user information (12.1), terminal information (8.7), and usage information (8.4) were analyzed as having a higher percentage of weight than in the existing work environment.

Table 9. Comparison of results of weighting analysis of existing and smart work environments.

Area		Weighting		Gap
		Existing Work Environment	Smart Work Environment	
Policy readiness	Outside the organization environment	37.2	32.4	−4.8
	Within the organization guideline	21.7	23.8	2.1
	Subtotal	**58.9**	**56.2**	-
Technical readiness	System information	13.0	9.7	−3.3
	Terminal information	5.7	8.7	3
	User information	10.7	12.1	1.4
	Usage information	6.2	8.4	2.2
	Additional function	5.5	4.9	−0.6
	Subtotal	**41.1**	**43.8**	-
	Total	**100.0**	**100.0**	-

Note: Areas with higher weight compared to existing work environment in smart work environment is marked in style "shade", major summary part is marked in style "bold".

The differences in the two environments were more pronounced in the technical readiness area than the policy readiness area. In particular, in the existing work environment, it was shown that system information used internally and additional function level were most important. Also, it was reported that device information utilized in outside the organization, user information which can distinguish a user when using a public devices and usage information which considers a characteristics of being able to utilize regardless of location and time are more important in the smart work environment where the work space is unconstrained due to cloud computing environment.

Through the validation and weight calculation, we eliminated the components with validities less than 3.5 and calculated the weights of each component. Finally, we designed the digital forensic readiness model of the cloud computing-based smart work environment (see Table 10).

Table 10. Digital forensic readiness model for cloud computing-based smart work environment (final).

Area (Weight)		Component and Description
Policy readiness	Outside the organization environment (32.4)	-Adhere to digital forensics related standards/guidelines: Secure integrity/reliability of digital evidence by adhering to digital forensics related standards/guidelines -Adhere to legal requirements: Adhere to legal procedure (secure suitability/objectivity) -Establish single contact point with law enforcement organizations: Establish single contact point with law enforcement organizations for continuous interactions regarding court cases
	Within the organization guideline (23.8)	-Prepare forensics solutions (proactive/detailed analysis tools): Secure proactive evidence collection system through preparation of forensics solution -Prepare forensics equipment (writing prevention devices, copiers, etc.): Secure proactive evidence collection system through preparation of forensics equipment -Identify and categorize information assets: Identify and categorize information assets for effective administration of information assets -Secure confidentiality agreements, etc.: Secure confidentiality agreements, etc. to reinforce organization members' security consciousness and responsibility -Establish evidence preservation system (server): Maintain safe preservation and integrity of original evidence through construction of evidence preservation system (server) -Use proven forensics tools: Secure the reliability/objectivity of forensic tools -Create an exclusive forensics department (personnel): Create an exclusive department (personnel) to conduct an effective digital forensic -Educate and train employees considering environmental change: Educate and train employees periodically to cope with rapidly changing environments -Establish evidence preservation policy: Maintain safe preservation and integrity of original evidence through the construction of an evidence preservation policy -Establish personnel audit policy: Secure legitimacy of internal audit
Technical readiness	System information (9.7)	-Analyze basic system information: Analyze the system environment by analyzing the basic system information -Analyze system on/off time: Analyze the system environment analysis by analyzing the system on/off time -Analyze the installed program breakdown: Analyze the system environment by analyzing the installed program breakdowns -Analyze the auto-execution program breakdown: Analyze the system environment by analyzing the auto-execution program list -Analyze the network information: Analyze the network environment such as IP/MAC Address and bandwidth -Analyze shared folder breakdown: Analyze the network environment such as shared folder breakdown -Analyze the external storage memory connection breakdown: Analyze the user's act of usage to confirm whether to use external storage memory -Analyze anti-forensic trace: Analyze the user's act of usage to confirm whether to conduct anti-forensic -Analyze virtualization environment construction trace analysis: Analyze the user's act of usage to confirm whether to construct a virtualization environment -Analyze the cloud service synchronization breakdown: Analyze the user's act of usage analysis to confirm whether to utilize the cloud service
	Terminal information (8.7)	-Collect/gain flash memory: Gain flash memory data for terminal analysis -Collect/gain microSD cards: Gain microSD cards data for terminal analysis -Collect/gain USIM cards: Gain USIM cards for terminal analysis -Collect/gain virtual machine image: Collect/gain virtual machine image for virtualization environment analysis in the case of virtualization environment-built terminals
	User Information (12.1)	-Analyze user account information: Analyze basic information on user account -Analyze visited website information: Analyze the user's website usage pattern -Analyze the portal search word: Analyze the user's website usage pattern -Analyze the recently opened document: Analyze the user's document data (local system) act of use -Analyze recently executed programs: Analyze the user's application program act of use -Analyze the executed command: Analyze the user's command act of usage -Analyze the user's used service: Analyze the user's service act of use
	Usage Information (8.4)	-Analyze Mobile OS (Android/iOS, etc.) artifact timeline: Analyze OS artifact timeline of primary mobile terminal -Analyze MAC file timeline analysis: Analyze the user's file usage pattern according to flow of time -Analyze action through the timeline: Analyze the user's action according to the flow of time -Apply a credible time stamp: Apply a credible time stamp to clearly confirm the flow of time
	Additional Function (4.9)	-Provide prompt file search: Provide file searches for prompt digital forensic performance -Search and analyze large files: Provide large file searches to analyze cloud computing servers retaining large files -Analyze the existence of unauthorized files: Provide searches to confirm if they are authorized -Search for encrypted files and decrypt: Provide searches for encrypted file analysis -Analyze hidden files by changing the extension: Provide searches for hidden files analysis -Derive hash values for searched files: Derive hash values to enhance search reliability

The digital forensic readiness model for cloud computing-based smart work environments that we formulated in this research is different to existing reactive digital forensic frameworks in the manner in which policy readiness was designed, including major components of proactive forensic activity

(see Table 11) such as digital forensic-related policy, standards, provision of guidelines, and educational training targeting the members of an organization.

Table 11. Major components of proactive forensic and reactive forensic activity.

Major components of proactive forensic activity	-Information Security Management & Evidence Management Framework (i.e., policies, standards, guidance) -Security awareness training (i.e., stakeholder, general user) Administrative, technical, physical control mechanisms (e.g., operating procedures, tools and equipment, specialized technical skills) -Organizational, regulatory, and legal compliance requirements
Major components of reactive forensic activity	-Incident response capabilities -Security incident response team (SIRT) -Computer (security) incident response team -Disaster recovery planning (DRP) -Business continuity planning (BCP) -Information security gap analysis and recommendations

Moreover, our model is differentiated from existing digital forensic readiness models in that three major areas—"terminal information", "user information", and "usage information"—were deduced by conducting an analytic hierarchy process analysis in order to determine the relatively more important components of digital forensic readiness in cloud computing-based smart work environments, compared to existing work environments (see Table 12).

Table 12. Major areas of digital forensic execution weighted according to their importance for different work environments.

Area	Weighting	
	Existing Work Environment	Smart Work Environment
System information	13.0	9.7
Terminal information	5.7	8.7
User information	10.7	12.1
Usage information	6.2	8.4
Additional function	5.5	4.9

Note: Areas with relatively higher weight in each work environment is marked in style "shade".

The principal areas of digital forensic execution may be grouped according to their environmental characteristics of cloud computing-based smart work environment and existing work environment, as illustrated in Figure 5.

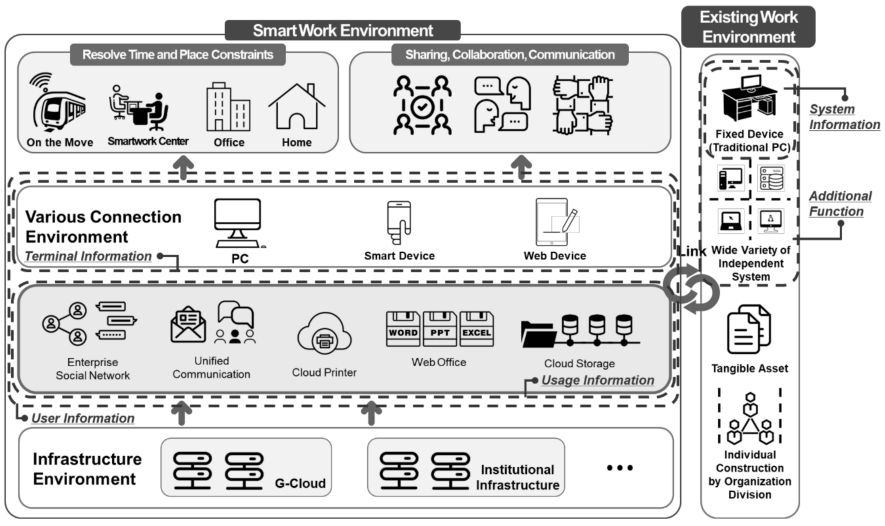

Figure 5. Major areas of digital forensic execution grouped according to environmental characteristics.

In particular, "terminal information" is a major area that enables rapid and effective digital forensic investigation through the user action analysis in the smart work environment where a high capacity of data is processed using various terminals based on cloud computing technology a variety of information in the terminal can be acquired. Figure 6 shows an analytical screen of mobile terminal using a digital forensic tool and detailed qualification of terminal such as model, memory, CPU and etc. of mobile terminal which is currently being analyzed can be confirmed. To conduct an effective digital forensic investigation, such digital forensic tool is used to understand model, qualification and etc. of terminal. Then internal storage device, such as flash memory, microSD card, etc., should be acquired by considering a characteristic of terminal.

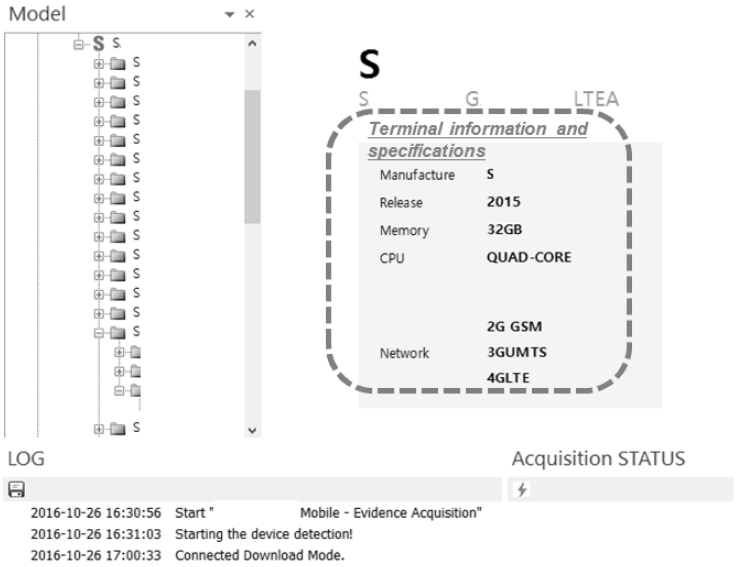

Figure 6. Confirmation of basic terminal information.

After acquiring the terminal storage memory, analysis of whether information has been leaked through the terminal, and whether the terminal users have conducted malicious actions should be performed. In the case of Android OS, which has highest OS share of current smart phone terminals, digital forensic tools can be utilized to confirm the database and attempt to restore a deleted record as shown in Figure 7. Attempts can be made to restore deleted files in the storage memory by file carving, as shown in Figure 7. Through the analysis of information within this storage memory, we can identify if illegally transferred important information assets were saved in the terminal.

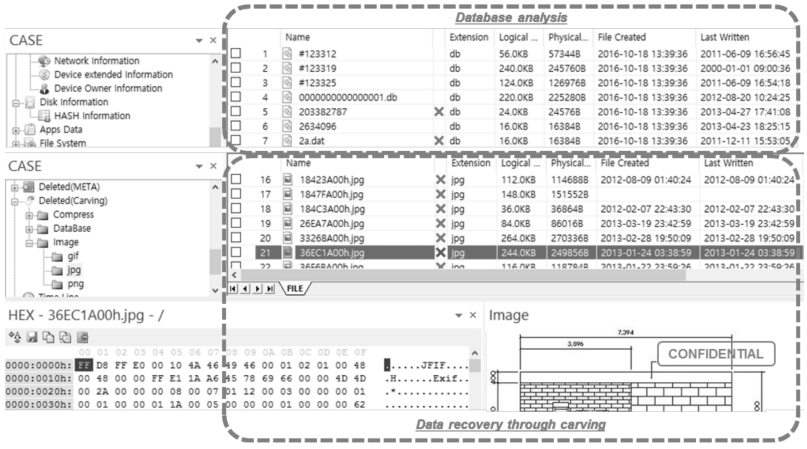

Figure 7. Analysis of internal storage analysis within the terminal.

However, even if important information assets were simply stored in the terminal, further investigation is required to understand if corresponding information assets were actually leaked externally, the leakage method, location to which it was leaked, etc. To analyze this, additional analysis of "user information" and "usage information" should be conducted. Figure 8 shows a display where records created in program (application) installed in the device and deleted records are being analyzed using a digital forensic tool. First of all, to analyze "user information", the digital forensic tool is used to analyze what behavior has occurred in which program through analysis of the program (application) installed in the device and relevant record analysis. Then, user information of those who actually used a device should be analyzed and an analysis conducted of moving routine regarding where and through what program important information about the asset has been leaked.

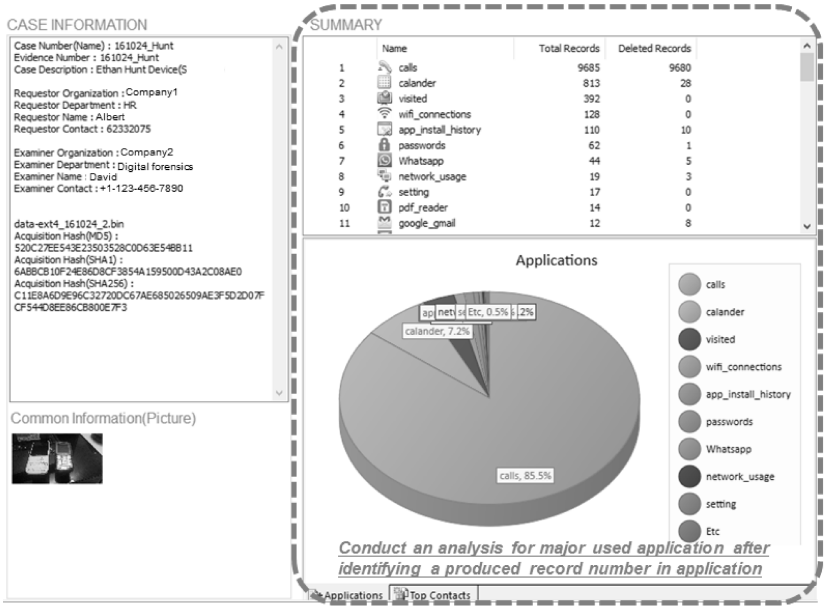

Figure 8. "User information" analysis through terminal analysis.

Additionally, simultaneous analysis of "user information" and an action analysis through the timeline of the "usage information" area facilitates comprehension of the leakage route of important assets. Action analysis through the timeline can be diversely utilized throughout the digital forensics process. Generally, digital forensic investigations can be conducted rapidly and effectively by identifying the terminal use time outside of business hours, or intensively collecting the time zone information where abnormal action is suspected by analyzing the system on/off time. Especially, if events happened according to the flow of time, as in Figure 9, and can be visualized into a scattered chart, this can be effectively used in detecting an abnormal action.

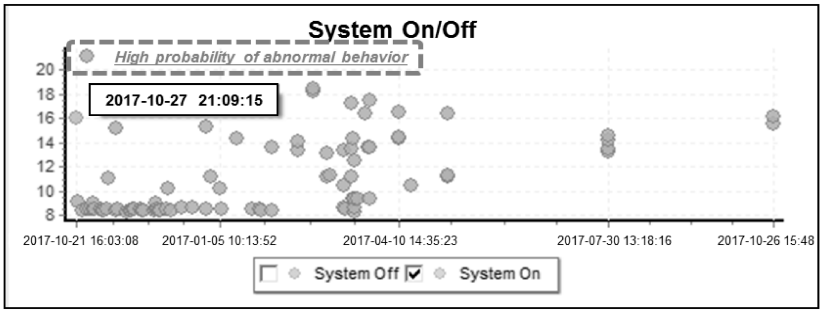

Figure 9. Action analysis through timeline.

If the digital forensic readiness model and digital forensic execution procedure using major components in the cloud computing based smart work environment are used, it is expected that we can effectively conduct a digital forensic investigation after an incident occurs, as well as building a proactive counterstrategy before an incident occurs.

4. Conclusions

We conducted research on digital forensic readiness procedures and structure models through the analysis of the literature related to digital forensic readiness, and examined the concept and characteristics of digital forensic readiness compared with security incident investigations that are centered on information protection.

In this research, we analyzed and identified the characteristics of the cloud computing-based smart work environment and, by reflecting these characteristics, we proposed component elements for the design of a digital forensic readiness model in the cloud computing-based smart work environment. In addition, to determine the validity of the corresponding model considering the cloud computing-based smart work environment, we conducted a validity analysis by collecting the survey data targeting digital forensic related experts. In addition, to analyze the weight by composition area proposed in this model, we calculated the weight by conducting an analytic hierarchy process analysis targeting digital forensic related experts. As a result, weighting in the areas of terminal information, user information, and usage information was shown to be higher than for existing work environments, which were analyzed for each organization to prepare for the components of digital forensic readiness of the corresponding area.

Unlike existing preemptive and inflexible work environments, the digital forensic readiness model deduced in this study can be applied in smart work environments where tasks are performed using various mobile devices based on cloud computing technology, which performs tasks without the constraints of time and space, and accelerates efficient information sharing with stakeholders. In addition, the corresponding digital forensic readiness model can be used in designing an anticipative and proactive counterstrategy before incidents occur; this model differs from traditional digital forensic approaches, which can be referred to as reactive actions, as they focus on collecting and analyzing evidence for victims after incidents occur.

In a cloud computing-based smart environment, the introduction of this digital forensic readiness can strengthen the overall level of internal information leakage prevention. By providing a foundation to secure the integrity of digital evidence, we expect that it will aid in establishing law and order, as well as prevent incidents of leaked internal information, by identifying and punishing malicious criminals.

From the perspective of the company, the digital forensic readiness system is expected to provide benefits by strengthening the risk management ability of the company, thereby minimizing damage from security incidents such as leakage of internal information and preventing secondary damage through swift security incident responses and other means.

However, when we evaluated the validity of the cloud computing-based smart work environment digital forensic readiness model proposed in this paper, not all evaluation criteria received scores that satisfied the validity, and the model is limited in that the verification of the reliability of the survey data was not included.

In future research, an in-depth analysis of the digital forensic readiness model in the cloud computing-based smart work environment is to be conducted for supplementation and greater validity. In addition, there should be further research that adds the characteristics of proactive, live, and reactive digital forensics for the digital forensic readiness area in the cloud computing-based smart work environment. Then, after distinguishing these, it is necessary to conduct in-depth recalculation of the weighting.

Acknowledgments: This work was supported by the Human Resources Development (No. 20174030201810, No. 20184030202070) of the Korea Institute of Energy Technology Evaluation and Planning (KETEP, Seoul 06175, Korea) grant funded by the Korea government Ministry of Trade, Industry and Energy.

Author Contributions: Sangho Park conducted the overall research processes and wrote the manuscript. Yanghoon Kim and Gwangmin Park conducted data analysis and wrote the manuscript. Onechul Na conducted preceding research analysis and data collection. Hangbae Chang developed the research framework and consulted on the manuscript development.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Baek, S.; Lim, J. A Study on the Forensic Readiness as an Effective Measure for Personal Information Protection. *Internet Inf. Secur.* **2012**, *3*, 34–64.
2. Elyas, M.; Maynard, S.B.; Ahmad, A.; Lonie, A. Towards a systemic framework for digital forensic readiness. *J. Comput. Inf. Syst.* **2014**, *54*, 97–105. [CrossRef]
3. Mell, P.; Grance, T. *The NIST Definition of Cloud Computing*; Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, United States Department of Commerce: Gaithersburg, MD, USA, 2011.
4. Boorsma, B.; Shane, M. *Work-Life Innovation: Smart Work—A Paradigm Shift Transforming How, Where, and When Work Gets Done*; Cisco Internet Business Solutions Group: San Jose, CA, USA, 2011.
5. Ministry of the Interior, Republic of Korea. *Cloud Work Environment Introduction Guide in Administrative Agency*; Ministry of the Interior: Seoul, Korea, 2016.
6. Software Policy & Research Institute. *Key Issue and Countermeasures in Cloud Security*; Software Policy & Research Institute: Gyeonggi, Korea, 2017.
7. Liao, Y.C.; Langweg, H. Evidential Reasoning for Forensic Readiness. *J. Digit. Forensics Secur. Law* **2016**, *11*, 37–52. [CrossRef]
8. Raghavan, S. Digital forensic research: Current state of the art. *CSI Trans. ICT* **2013**, *1*, 91–114. [CrossRef]
9. Elyas, M.; Ahmad, A.; Maynard, S.B.; Lonie, A. Digital forensic readiness: Expert perspectives on a theoretical framework. *Comput. Secur.* **2015**, *52*, 70–89. [CrossRef]
10. Dezfoli, F.N.; Dehghantanha, A.; Mahmoud, R. Digital Forensic Trends and Future. *Int. J. Cyber-Secur. Digit. Forensics* **2013**, *2*, 48–76.
11. Lee, C.H. Digital Forensics Framework for Cloud Computing. *J. Adv. Navig. Technol.* **2013**, *17*, 63–68. [CrossRef]
12. Sachowski, J. *Implementing Digital Forensic Readiness: From Reactive to Proactive Process*; Syngress: Cambridge, MA, USA, 2016; pp. 45–153. ISBN 9780128044544.
13. Endicott, B.; Popovsky, N.K.; Rudolph, C. Forensic Readiness: Emerging Discipline for Creating Reliable and Secure Digital Evidence. *J. Harbin Inst. Technol.* **2015**, *22*, 1–8.
14. Rafique, M.; Khan, M.N.A. Exploring static and live digital forensics: Methods, practices and tools. *Int. J. Sci. Eng. Res.* **2013**, *4*, 1048–1056.
15. Kim, J.; Son, Y.; Chung, M. A Design of Evaluation Framework for the Assets and Insolvency Prediction Depending on the Industry Type Using Data Standardization based on the Forensic Readiness. *Int. J. Multimedia Ubiquitous Eng.* **2015**, *10*, 345–354. [CrossRef]
16. Hale, J.S. Amazon cloud drive forensic analysis. *Digit. Investig.* **2013**, *10*, 259–265. [CrossRef]
17. Al-Mahrouqi, A.; Abdalla, S.; Kechadi, T. Cyberspace Forensics Readiness and Security Awareness Model. *Int. J. Adv. Comput. Sci. Appl.* **2015**, *6*, 123–127. [CrossRef]
18. Kebande, V.R.; Venter, H.S. Novel digital forensic readiness technique in the cloud environment. *Aust. J. Forensic Sci.* **2017**, 1–40. [CrossRef]
19. Reddy, K.; Venter, H.S. The architecture of a digital forensic readiness management system. *Comput. Secur.* **2013**, *32*, 73–89. [CrossRef]
20. Kohn, M.D.; Eloff, M.M.; Eloff, J.H. Integrated digital forensic process model. *Comput. Secur.* **2013**, *38*, 103–115. [CrossRef]
21. Tot, L.; Grubor, G.; Marta, T. Introducing the Information Security Management System in Cloud Computing Environment. *Acta Polytech. Hung.* **2015**, *12*, 147–166.
22. Daryabar, F.; Dehghantanha, A.; Udzir, N.I.; Mohd Sani, N.F.; Shamsuddin, S.; Norouzizadeh, F. A Review on Impacts of Cloud Computing on Digital Forensics. *Int. J. Cyber-Secur. Digit. Forensics* **2013**, *2*, 77–94.

23. Almulla, S.A.; Iraqi, Y.; Jones, A. A state-of-the-art review of cloud forensics. *J. Digit. Forensics Secur. Law* **2014**, *9*, 7–28. [CrossRef]
24. Valjarevic, A.; Venter, H.S. A comprehensive and harmonized digital forensic investigation process model. *J. Forensic Sci.* **2015**, *60*, 1467–1483. [CrossRef] [PubMed]
25. Van Beek, H.M.A.; van Eijk, E.J.; van Baar, R.B.; Ugen, M.; Bodde, J.N.C.; Siemelink, A.J. Digital forensics as a service: Game on. *Digit. Investig.* **2015**, *15*, 20–38. [CrossRef]
26. Ruan, K.; Carthy, J.; Kechadi, T.; Baggili, I. Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results. *Digit. Investig.* **2013**, *10*, 34–43. [CrossRef]
27. Bashir, M.S.; Khan, M.N.A. Triage in live digital forensic analysis. *Int. J. Forensic Comput. Sci.* **2013**, *1*, 35–44. [CrossRef]
28. Martini, B.; Choo, K.K.R. Cloud storage forensics: Own Cloud as a case study. *Digit. Investig.* **2013**, *10*, 287–299. [CrossRef]
29. Pichan, A.; Lazarescu, M.; Soh, S.T. Cloud forensics: Technical challenges, solutions and comparative analysis. *Digit. Investig.* **2015**, *13*, 38–57. [CrossRef]
30. Quick, D.; Choo, K.K.R. Google drive: Forensic analysis of data remnants. *J. Netw. Comput. Appl.* **2014**, *40*, 179–193. [CrossRef]
31. Quick, D.; Choo, K.K.R. Impacts of increasing volume of digital forensic data: A survey and future research challenges. *Digit. Investig.* **2014**, *11*, 273–294. [CrossRef]
32. Dlamini, M.; Venter, H.; Eloff, J.; Eloff, M. Requirements for Preparing the Cloud to Become Ready for Digital Forensic Investigation. In Proceedings of the European Conference on Cyber Warfare and Security, Piraeus, Greece, 3–4 July 2014; pp. 242–250.
33. Shah, J.; Malik, L.G. Cloud forensic issues and challenges. In Proceedings of the International Conference on Emerging Trends in Engineering and Technology, Bucharest, Romania, 19–21 September 2013; pp. 138–139.
34. Damshenas, M.; Dehghantanha, A.; Mahmoud, R.; Shamuddin, S.B. Cloud computing and conflicts with digital forensic investigation. *Int. J. Digit. Content Technol. Appl.* **2013**, *7*, 543–553.
35. Lee, G.M.; Lee, Y.S. Digital Forensic Model Suitable for Cloud Environment. *J. Inf. Secur.* **2017**, *17*, 15–20.
36. Tavakol, M.; Dennick, R. Making sense of Cronbach's alpha. *Int. J. Med. Educ.* **2011**, *2*, 53–55. [CrossRef] [PubMed]
37. Lee, J.H.; Cho, S.H. An Analysis on the Problems of Design Competition Process of Landscape Architecture by the Delphi Analysis Method. *J. Korean Inst. Landsc. Arch.* **2013**, *41*, 83–93. [CrossRef]
38. Nam, S.T.; Jin, C.Y.; Kim, D.G. Preference Analysis for Location Based Services on Smartphone Environment Using Analytic Hierarchy Process. *J. Korea Inst. Inf. Commun. Eng.* **2014**, *18*, 1337–1342. [CrossRef]