Journal of Computer Science 6 (6): 613-618, 2010
ISSN 1549-3636

Adopting Hadith Verification Techniques in to Digital Evidence Authentication

Yunus Yusoff, Roslan Ismail and Zainuddin Hassan
Department of Software Engineering, College of Information Technology,
University Tenaga National, 43009 Kajang, Selangor, Malaysia

Abstract: Problem statement: The needs of computer forensics investigators have been directly influenced by the increasing number of crimes performed using computers. It is the responsibility of the investigator to ascertain the authenticity of the collected digital evidence. Without proper classification of digital evidence, the computer forensics investigator may ended up investigating using untrusted digital evidence and ultimately cannot be use to implicate the suspected criminal. **Approach:** The historical methods of verifying the authenticity of a hadith were studied. The similarities between hadith authentication and digital evidence authentication were identified. Based on the similarities of the identified processes, a new method of authenticating digital evidence was proposed, together with the trust calculation algorithm and evidence classification. **Results:** The new investigation processes and an algorithm to calculate the trust value of given digital evidence was proposed. Furthermore, a simple classification of evidence, based on the calculated trust values was also proposed. **Conclusion/Recommendations:** We had successfully extracted the methods to authenticate hadith and mapped it into the digital evidence authentication processes. The trust values of digital evidence were able to be calculated and the evidence can be further classified based on the different level of trust values. The ability to classify evidence based on trust levels can offer great assistance to the computer forensics investigator to plan their works and focus on the evidence that would give them a better chance of catching the criminals.

Key words: Computer forensics, digital evidence authentication, hadith authentication

INTRODUCTION

We are experiencing the explosive growth of the usage of computers in our daily lives, may it be at the personal or corporate levels. A great deal of companies and other organizations are using computers to conduct their businesses. While the astonishing usage of computer facilities and services has brought about great benefits to us, it has also inadvertently attracting attention of the criminals. The needs of computer forensics investigators have been directly influenced by the increasing number of crimes performed using computers. Investigators would be required to analyze the digital evidence with the objective to identify the suspected criminals. It is the responsibility of the investigator to ascertain the authenticity of the collected digital evidence. Unless the evidence can be proven to be authentic and reliable, it would be meaningless to present it in the court of law. As such, it is of a paramount important for the forensic investigator to conduct the investigation process properly and based on acceptable practices.

Carrier and Spafford (2002); Noblett *et al*. (2000); Baryamureeba and Tushabee (2006) and Rogers *et al*. (2006) have discussed various techniques to conduct computer forensic investigations. Based on their discussions, it is apparent that the computer forensic investigation processes have many areas that can be further improved, especially in the area of digital evidence authentication.

We are taking this opportunity to propose a digital investigation techniques derived from extensive work done in another domain i.e., hadith authentication. Our earlier works has been primarily focused on the methodology used by the authenticator of hadith. We have great expectation that the hadith authentication techniques that were developed and improved for over 1000 years ago and stand the test of times can be used to contribute to the body of knowledge in the digital authentication processes.

Hadith is referred to the words, deeds, tradition, silent approval and personality of Prophet Muhammad S.A.W. (peace be upon him) (Mahmood, 2006). Ahadith (plural form of a hadith) are regarded as the

Corresponding Author: Yunus Yusoff, Department of Software Engineering, College of Information Technology, University Tenaga National, 43009 Kajang, Selangor, Malaysia

2nd authority in Islam after the Al-Quran (Ali, 1996). The people who recorded the hadith, known as muhadith, took a great deal of care when recording and transmitting a hadith. Not only do they look at the content, but also at the people who narrated the hadith. Nevertheless, in the process of acquiring, transmitting and recording the life and conduct of the Prophet S.A.W., the muhadith may have unintentionally committed some mistakes (Yusoff *et al*., 2008). To make matters worse, there exist devious people who purposely modify and introduce new materials purportedly connected to the Prophet S.A.W. Therefore, the science of hadith was introduced, to ascertain the correctness of every single statement attributed to the Prophet S.A.W. (Azami, 1977).

Hadith consist of two parts (Fig. 1) i.e., matn (content) and isnad (the sequence of people who narrated the hadith). In digital realm, matn can be equated to the actual data and isnad can be equated to the path or channel the data is obtained or transmitted.

Mapping of hadith authentication onto digital investigation processes: It has been noted that there exist direct similarities between hadith authentication and digital evidence authentication. The similarities can be observed in the following areas namely content verification, transmitters' reliability, transmission's reliability and change of custody.

Content verification: Hadith authentication requires for the verification of its matn (content). Scholars of hadith study, known as muhadithin, have indeed paid meticulous attention to ascertain the validity of the content of a hadith.

In confirming that the matn is valid, the muhadithin employed various techniques. For example, if the content of the hadith contradicted the teaching of Al-Quran, it is then classified as maudu' (false/fabricated) and be automatically rejected.

Prophet S.A.W. spoke using the words that were normally used by the people during his lifetime. Otherwise, it would be difficult for the people to understand and comprehend what the Prophet S.A.W. said. Therefore, if the words recorded in the hadith are unfamiliar and not normally used by the community during the lifetime of the Prophet S.A.W. then the validity of such hadith can be questioned.

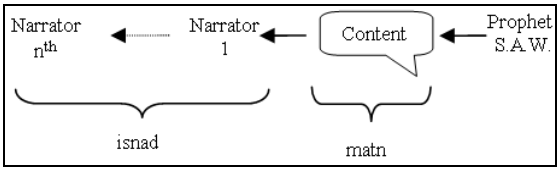

Fig. 1: Hadith component (Yusoff *et al*., 2008)

The actions described in the hadith must not go against the known behavior of Prophet S.A.W. Such hadith that record un-prophet-like conducts will be automatically rejected.

In digital evidence investigation, there exist methods to verify that a text is produced/derived from an individual. The author identification techniques (Chaski, 2005), based on stylometric characteristics are among the various techniques that can be used to verify whether a document is indeed written/produced by the accused. The idea behind this technique is based on the fact that individuals have their own unique style of writing. It is possible to ascertain the original author of a document by analyzing certain characteristics embedded in a document, such as language style, notation used, verbs used.

Based on hadith authentication methodology, if for example, the matn contains a vulgar expression or contradictory to the characteristic of Prophet Muhammad S.A.W., the hadith will be immediately rejected without the consideration of the isnad (Suhaib, 2008). Therefore, once the matn check can be proven beyond reasonable doubt that the suspect is not the author of the email the checking of isnad (transmitter and transmission of the email) would no longer be required.

Reliable transmitter: Even though, the content of a hadith looks acceptable and does not contradict with Al-Quran and the Prophet S.A.W., it is not guaranteed that it is genuine. It must be proven that it has been transmitted by the reliable transmitters. For every hadith, there must be a list of transmitters that can be traced all the way back to the Prophet S.A.W.

It is very important for the transmitter to demonstrate that he is capable to recite and transmits the hadith accurately. He should also be proven to have a good retention of memory. Most of the hadith transmissions during the early times were done primarily via the verbal transmission based purely from memory of the narrators (Mahmood, 2006). The transmitters must also be known to have lived a righteous life. Failure of any of the transmitter to adhere to these criteria can make the hadith to be questionable and would bring down the level of validity of the particular hadith.

A clear case of forgery by the transmitter would render the transmitted hadith to be outright rejected (Azami, 1977).

Reliable transmission method: Not only the narrator is subjected to scrutiny, the way the narrator transmits the hadith to another narrator is equally important and

heavily scrutinized. It will bring disrepute to the hadith if the narrator was confirmed to be acceptable, but the method of transmission was not reliable or questionable.

One of the hadith transmission criteria is that the transmitter and receiver must live in the same time period. It would be a gross injustice to accept a hadith whereby the transmitter live in one period and the receiver live in a period after the death of the transmitter.

In addition to the same lifetime period, the receiver must also be at a rescannable age range to receive a hadith. If the age of the receiver is too young, the transmitted hadith can still be questionable.

Relating to digital evidence investigation, the above methods can be equated to the way data is transmitted from one location to another. The investigator needs to ensure that it is indeed possible for the data to move from one component to another, such as images to be transferred from one mobile device to another. The transmission path and the opportunity for the digital transmission to take place must be available. The date of sending and the date of receiving must also be reasonable, so that the possibility of transmission can be acknowledged.

In addition to the reasonable transmission timeframe, the capacity/ability of the receiving component must also be examined. If the image size is 1 GB and the size of the memory on the particular hand phone is only 512 MB, it is then safe to conclude that the transmission via that hand phone does not take place.

Proper change of custody: In digital evidence investigation, maintaining a proper change of custody is a very important criterion that all investigators must adhere to. Throughout the lifecycle of the investigation, the record of the evidence custodianship must be properly kept. Without the proper custodianship it cannot be ascertained that the evidence has not been tainted.

The isnad system, by virtue of its concept and implementation, is similar to the concept of chain of custody. For a hadith to be accepted, it must have an unbroken and reliable link of narrators all the way back to the Prophet S.A.W. The strength of the link does depend on the strength of all of the narrators in the link. Any weakness to any one of the narrators would ultimately weaken authenticity level of the hadith (Azami, 1977).

Similarly in digital forensic realms, any weakness in any part of the chain of custody would render the evidence to be atrociously challenged in the court of law.

MATERIALS AND METHODS

Inline with hadith authentication scenario, we need to state our assumption that the source of the evidence is known. The ultimate objective is to authenticate that the evidence is indeed derived from the suspected source. Yusoff *et al*. (2008) have demonstrated, a surface level scenario, as to how the technique to check for matn and isnad can be applied into the checking of an email coming from a suspected criminal.

Figure 2 demonstrates the email investigation process based on hadith authentication method.

The process started when the victim produced an email purportedly sent by the accused. The first step is to check for the validity of the content, which is the matn checking. If it can be proven that it is impossible for the accused to have written such email, the investigation process stops and the accused is no longer implicated. Email matn check can be done via various techniques such as authorship verification and digital signatures. If the matn check showed a positive result that indicated for the possibility of the accused to have written such email, the next step is to check for the isnad's validity. The checking for the isnad must cover all transmitters starting from the receiver until the source transmitter. These transmitters must be in a continuous and unbroken chain.

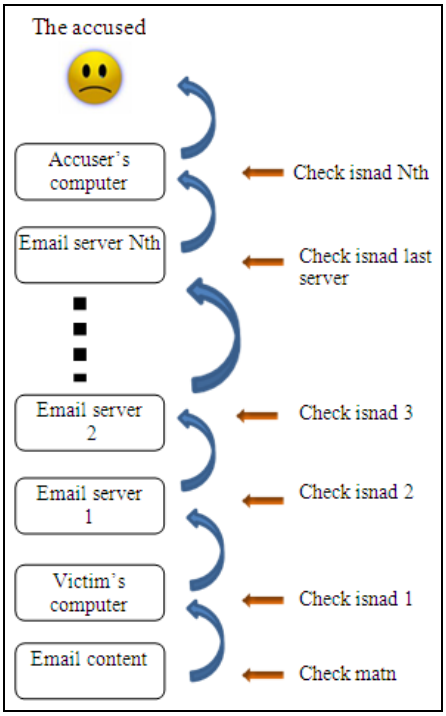

Fig. 2: Email investigation process

This isnad checking would encompass the verification and authentication of the receiver's computers, all email processing and forwarding servers and finally, the accused computer. There are various techniques currently available to check for the isnad of the email such as analysis of the email header to ascertain the path and existence of the email server(s).

It is difficult to get a clear/concrete yes or no answers for both matn and isnad checking. After all, representing trust values in binary format (yes or no) would be too simplistic and unable to represent the true value of trust satisfactorily (Li and Singhal, 2007). As such, we are proposing for the trust values of the range between 0 (completely untrusted) and 1 (completely trusted), be assigned for each of the checks. The overall trust value for digital evidence (in this case, an email sent by the accused to the victim) can be calculated based on the proposed formula:

$$T(x) = 0.5*M(x) + 0.5*I(x)$$
$$\text{If } M(x) = 0 \text{ or } I(x) = 0, \text{ thus } T(x) = 0 \quad (1)$$

$T(x)$ = The trust value of evidence x
$M(x)$ = The trust value of matn check performed on x
$I(x)$ = The trust value of isnad check performed on the transmitters of x

The trust value of evidence x is the sum of 50% of the trust of matn x and 50% of the trust on isnad x. This is done to show that both matn and isnad checks carries the same weightage. However, should any of the values become 0, the entire formula will be 0, thus the trust value of the evidence x will also be 0 (totally untrusted). If the content check reveals 0 trusts, then there is no need to check the transmission path as the resulting trust value should be zero. The same goes if the value of the transmission path is equals to 0. Should both values become 1, the result of the formula will be 1, thus the trust value of evidence x will also be 1 (completely trusted). M(x) and I(x) of any value between 0 and 1 would bring about the trust values ranging between 0 and 1.

The calculation of M(x) would be based on the authorship identification techniques. One such technique is making use of stylometry, which assume that an author has distinctive writing habits and these are exhibited in features like vocabulary used, sentence complexity and phrases used. Since the suspect of the email author is known, it is possible to get copies of previous emails or other text written by the suspect. Using the known text and the text in the email in investigation, it is possible to calculate the trust value of M(x) using any of the currently available authorship identification techniques (Anderson *et al*., 2001; De Vel *et al*., 2001).

Based on isnad calculation, the formula for I(x) can be further expanded into the following:

$$I(x) = \text{MIN } \{I(x_1), I(x_2),\ldots, I(x_n^{th})\} \quad (2)$$

The calculation of I(x) is composed of $I(x_1)$, $I(x_2)$ until I (x_n^{th}), the source transmitter. It is important to note that the trust value of I(x) is based on the lowest value in the chain. This is indeed in line with the hadith authentication concept whereby the strength of the entire chain is the strength of its weakest link.

As for the calculation of each $I(x_i)$, we proposed that the value of $I(x_i)$ is based on the penetration test performed on server plus the history of penetration test on the server:

$$I(x_i) = (Pt(x_i) * 0.7) + (Ph(x_i) * 0.3)$$
$$\text{If } Pt(x_i) = 0, \text{ thus } I(x_i) = 0 \quad (3)$$

$Pt(x_i)$ = The penetration test value on server i
$Ph(x_i)$ = The history of penetration test values done on server i

The discounted rate of 70% is imposed on value of $Pt(x_i)$ and only 30% is imposed on the value of $Ph(x_i)$. This is to reflect the higher importance of the current penetration test values as compared to the historical values. However, if the current penetration test value is equivalent to 0 (totally entrusted), it is safe to assume that the combine trust of $Pt(x_i)$ and ($Ph(x_i)$ should also be 0.

Server that passed all current penetration tests would be considered as achieving the trust value of 1 for $Pt(x_i)$. $Ph(x_i)$ is the storage place for all penetration tests done on server i. $Ph(x_i)$ will be continuously updated whenever a new penetration test is done on server i.

Similarly with the hadith authentication methodology, other than checking the matn and reliability of the transmitter(s) in the isnad chain, the way the hadith being transmitted is also equally scrutinized. As such, the transmission of email being investigated from the sender to the recipient must also be looked into. With the widely available mobile devices such as notebooks, PDAs, smart-phones, it is quite possible for the data under investigation to have passed through these devices via wireless communication. As such the formula for calculation of email isnad can be further extended to:

$$I(x_i) = 0.5((Pt(x_i) * 0.7) + (Ph(x_i) * 0.3)) + 0.5((Tt(x_i) * 0.7) + (Th(x_i) * 0.3))$$
$$\text{If } Pt(x_i) = 0 \text{ or } Tt(x_i), \text{ thus } I(x_i) = 0 \quad (4)$$

$Tt(x_i)$ is the trust value of the transmission test between server (i+1) and server I and $Th(x_i)$ is the historical value of the transmission test done on the same two servers. It is important to note that the combination values of $(Pt(x_i) + Ht(x_i))$ and $Tt(x_i) + Th(x_i)$ are averaged out in order to reflect the same level of important between the server reliability and the transmission reliability. However, should $Tt(x_i)$ be 0, the whole $I(x_i)$ value will be set to 0. This is in line with the concept that for an evidence to be accepted, it should be reliably transmitted. Should the reliability of the transmission is 0 (not trusted at all), the evidence should be rejected.

As such, the complete formula for the trust of digital evidence x is as follows:

$$T(x) = 0.5*M(x) + 0.5*I(x)$$

Whereby:

$$I(x) = MIN \{I(x_1), I(x_2),\ldots, I(x_n^{th})\}$$
$$I(x_i) = 0.5((Pt(x_i) * 0.7) + (Ph(x_i) * 0.3)) + 0.5((Tt(x_i) * 0.7) + (Th(x_i) * 0.3)) \quad (5)$$

The resulting trust value will be between 0 and 1. Zero being completely untrusted and 1 being fully trusted. When confronted with numerous evidences, the forensic investigator can rank those evidences based on the calculated trust values. The evidence that achieved high trust value (for example 70% or more) can be safely used as evidence in the court of law. This ranking of evidence can assist the forensic investigator to prioritize which evidence that they can further investigate and which ones that they can put on hold or discard altogether. Being able to classify the evidences based on the level of trusts would enable the investigators to efficiently utilize their investigation time.

Trust classification: In general, hadith can be classified into 4 categories (Mustafa, 2005) or trust levels namely, Sound (Sahih), Good (Hassan), Weak (Daif) and Bad/Rejected (Maude'). Based on the hadith classifications and mapping it to the calculated trust values, we propose the following classification of the digital evidence:

Level 4: Sound: The trust value of 1.0
Level 3: Good: The trust value of > 0.7
Level 2: Weak: The trust value of > 0.3
Level 1: Bad: The trust value of <= 0.3

The ability to classify the evidence based on the above proposed classifications would enable the forensic investigators to plan their works and focus on the evidence that would give them a better chance of catching the criminals. The evidence that falls under into the lower level trust category can be disregarded or ignored at least for the time being. The investigators can come back later to these low trust level evidences and use them to provide leads and clues to other evidences.

The above trust classifications are still raw and will be subjected to further refinements. We should be able to substantiate and finalize the classifications once we have completed our work on the testing of the case studies.

RESULTS AND DISCUSSION

Employee A has received a threatening email from Employee B. Employee B has denied ever sending such email. A computer forensic investigator was called in to investigate the matter (Fig. 3).

Based on the initial investigation from the email headers and tracing back to the source, the following email transmission path was discovered.

In order to ascertain the trust of the threatening email evidence, the investigator has applied the trust formula i.e.:

$$T(x) = 0.5*M(x) + 0.5*I(x)$$

First of all, the value of M(x) is calculated using authorship identification techniques. The calculated value is then converted to the trust value of between 0 and 1.

Assuming that the value of M(x) = 0.25, which is>0, the value of I(x) is then be calculated, starting with Mary's PC and go all the way to John's notebook. At each of the node/isnad, the penetration test $Pt(x_i)$, history test $Ht(x_i)$ and transmission test $Tt(x_i)$ are performed. Assuming that the values of $Pt(x_i)$, $Ht(x_i)$ and $Tr(x_i)$, have already been calculated, the trust value at each node, $I(x_i)$, can then be derived, as shown in Table 1.

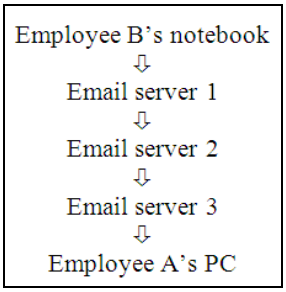

Fig. 3: Email path

Table 1: Intermediate trust values

x	Pt (x_i)	Ht (x_i)	Tt (x_i)	Th(x_i)	I (x_i)
1	0.80	0.90	0.70	0.7	0.77
2	0.35	0.10	0.10	0.8	0.29
3	0.70	1.00	0.60	0.9	0.74
4	0.90	0.80	0.80	0.5	0.79
5	0.30	0.50	0.60	0.8	0.51

As such, the trust value of evidence x (email from John to Mary) is then calculated as follows:

$$
\begin{aligned}
T(x) &= 0.5*M(x) + 0.5*I(x) \\
&= (0.5*0.25)+(0.5*\text{MIN } \{0.77, 0.29, 0.74, 0.79, 0.51\} \\
&= 0.125+0.145 \\
&= 0.27
\end{aligned}
$$

As such, the evidence can be classified as bad as it only obtains a trust value of 0.27 (which is less than 0.30). It is therefore, unlikely that John has send Mary the purported threatening Email. The computer forensic investigator can disregard or put on hold the investigation using this piece of evidence. They can focus on other evidence that have higher trust values in their quest to prove that John did indeed send the email.

CONCLUSION

We are able to present a noble way of calculating the trust value of a given email based on hadith authentication techniques. Even though the calculation presented is based on email domain, this formula can be used on other types of evidences. The concept of matn and isnad is general enough to be applied in authenticating various types of digital evidence. The development of case studies based on actual computer forensic investigations is the focus of our current work. A proper classification of the evidence based on the hadith classification such as sahih (fully accepted), hassan (slightly below sahih), dhaif (weak) and maudu (rejected). The next step is to formulate a realistic case scenario so that an acceptable and reasonable trust values can be assigned to matn and isnad checking. This framework can then be applied into digital evidence investigation to assist in ascertaining the trustworthiness of any given digital evidence.

REFERENCES

Azami, M.M., 1977. Studies in Hadith Methodology and Literature. American Trust Publication, ISBN: 983-9154-21-4, pp: 81-84.

Ali, M., 1996. Hadith and Sunnah. Islamic Book Trust, Kuala Lumpur, ISBN: 983-9154-02-8, pp: 23.

Anderson, A., M. Corney, O. De Veland and G. Mohay, 2001 . Identifying the Authors of Suspect Email, Computers and Security. http://eprints.qut.edu.au/8021/1/CompSecurityPaper.pdf

Carrier, B. and E.H. Spafford, 2002. Getting physical with the digital investigative process. Int. J. Digit. Evid., Fall, 1: 1-20.

Baryamureeba, V. and F. Tushabee, 2006. The enhanced digital investigation process model. Asian J. Inform. Technol., 5: 790-794.

Chaski, C.E., 2005. Who's at the keyboard authorship attribution in digital evidence investigations. Int. J. Digit. Evid., 4: 1-13.

De Vel, O., A. Anderson, M. Corney and G. Mohay, 2001. Mining e-mail content for author identification forensics. ACM SIGMOD Rec., 30: 55-64.

Li, H. and M. Singhal, 2007. Trust management in distributed systems. Computer, 40: 45-53. DOI: 10.1109/MC.2007.76

Mahmood, K., 2006. Hadith and Its Literary Style. Adam Publishers and Distribution, New Delhi, ISBN: 81-7435-474-3, pp: 11-28.

Mustafa, A.R., 2005. Hadith 40 (Translation of 40 Hadiths by Imam Nawawi). Dewan Pustaka Fajar, Kuala Lumpur, ISBN: 967-83-0058-3, pp: 19-24.

Noblett, M.G., M.M. Pollitt and L.A. Presley, 2000. Recovering and examining computer forensic evidence. Forensic Sci. Commun., 2: 1-8.

Rogers, M.K., J. Goldman, R. Mislan, T. Wedge and S. Debrota, 2006. Computer forensics field triage process model. Proceeding of the Conference on Digital Forensics Security and Law, pp: 27-40.

Suhaib, H., 2008. An Introduction to the Science of Hadith. http://www.usc.edu/dept/MSA/fundamentals/hadithsunnah/scienceofhadith/acov.html

Yusoff, Y., R. Ismail, M.Z. Mohd Yusof and A.A. Mat Isa, 2008. Conceptual similarities between hadith authentication and digital evidence verification techniques. Proceedings of the 4th International Conference Information Technology and Multimedia, UNITEN, Malaysia, pp: 192-196.