International Journal of Engineering & Technology, 7 (4.31) (2018) 74-79

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Enhanced Bring your Own Device (BYOD) Environment Security based on Blockchain Technology

Fara Jamal[1]*, Mohd. Taufik Abdullah[2], Azizol Abdullah[3], Zurina Mohd. Hanapi[4]

Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, 43400 Serdang, Selangor,Malaysia
**Corresponding author E-mail: f4ra.jamal@gmail.com*

Abstract

BYOD is a practice by many organizations where employees can use their personal devices for work purpose. BYOD may bring a lot of advantages, but it also leads to security issues such as data leakages. Data can be leaked because of the weak authentication technique used to verify the user and the device. A secure authentication technique is what the organization needs that equip with high security features. Blockchain is the answer to this because blockchain used cryptographic technology that's not easy for hacker to break. This research proposes a user trust model that includes multifactor authentication combining with public and private key generated by blockchain and an agentless device trust model that can scan for malware and detect the device location. In order to secure the record and sensitive data, the record keeping model is built using blockchain technology where every activity related to the record is recorded in the digital ledger. This ledger can be used as evidence collection for further investigation. It is hoped the proposed BYOD trust model solution can help organizations to minimize the number of cases in data leakage while allowing BYOD concept.

Keywords: *Authentication; Blockchain; BYOD; Data Leakage.*

1. Introduction

Bring Your Own Device (BYOD) has started to discuss in 1990 but only emerging in 2011. Until now the word BYOD is very common to organization in every country. Many organizations implement BYOD in order to enhance their computing resources, especially in term of hardware. It believes that BYOD actually increase employee productivity.

BYOD technology is relying on the Internet or network to communicate. This type of technology is easier to breach compare to previous technology such as mainframe, stand-alone system or client-based [1]. According to [2], once the organization data are allowed to be visited by the employees' personal devices, an organization loses the physical control over their data. In this century, data become a new currency and people are willing to pay for a huge amount of money to get data for their own used. As long as there is a market, and there are people willing to pay, there will be somebody somewhere who will be willing to take a risk and sell it. In order to sell the data, somebody must get access to the data or information from within an organization and transfer it to an external destination or recipient without authorization.

According to [3] this act is defined as data leakage. Data leakage can be accomplished by simply mentally remembering what was seen, by physical removal of tapes, disks and reports or by subtle means such as data hiding. With the emerging used of BYOD technology, data leakage becomes more common and harder to control since everybody can bring his or her personal device and connected to organization environment freely [4].

There are a few cases on data leakage involving big company reported. In 2013, three billion Yahoo account and data was compromised. In March 2017, hackers claim they breach apple iCloud that involves 250 million AppleIDs and demand for ransom from Apple. In October 2017, US-based score rating agency, Equifax were breached and the hackers stole over 145.5 million customer information ranging from credit report, personal identification numbers and even credit card details. Other cases happen also in October 2017 where more than 30 million citizens of South Africa personal data are leaked on the Internet placing them at risk of identity theft. In Malaysia, recently MCMC is still investigating on the data leakage report by lowyat.net that millions of personal data of Malaysian citizen are up for sale.

According to [5], one of the causes of data leakage is because of data are kept centralize. User data such as their ID, password, identity card number and personal information that are used for authentication are kept in one centralize server. The problem of centralize storage is, it can be a single point of failure [6]. Hackers can get access to the server and leak all the data inside. Cybercriminal can attack the server and stole the user ID and password. Legitimate users can access the server, stole the data, hand over to unauthorized personal without anybody know it. Centralize storage is a pull base technology where data are stored in one location and anybody can pull the data. Most of the organizations that allow BYOD stored their sensitive information in a centralized server. Even though organization implement authentication technique where only legitimate user can access the server, but still it is centralizing and easy to compromise. Anybody can pull the data anytime, keep it on their mobile phone, and sell it without anyone knowing it.

In order to secure the data from leakage, a proper solution will have to be created, and a blockchain-based approach would overcome many of the problems associated with the centralized approach [7]. Blockchain is a push technology where data are stored decentralize comparable to a centralize pull technology currently being used [8]. However, blockchain technology is still not fully mature and in the development stage which prone to many risks. Blockchain need to be combined with authentication technique because the blockchain timestamping does not prove ownership

[8]. Traditional way of authenticating that relied on either knowledge ownership is too weak for preventing data leakage in BYOD environment [9]. A user trust based authentication and a device trust based authentication needed to secure BYOD environment while storing the sensitive data in a blockchain environment.

Our Contribution. 1) Implement user trust model authentication includes ID, password, public key and private and device trust model authentication with agentless malware scanning and location detection for employee who want to access organization resources using their personal device. 2) Implement secure record keeping technique using blockchain technology that integrate with existing database 3) Enhance the digital ledger to make it as evidence collection 4) Discuss on the existing issue in data leakage and the used of blockchain in the literature review.

Organization. Section 2 is a Literature Review on data leakage and blockchain; section 3 provides an overview of our architecture; section 4 discusses future extensions to blockchains, and concluding remarks are found in section 5.

2. Literature Review

2.1. Data Leakage

Many researchers have different opinion on the worst threat in BYOD faced by organizations. Based on 80 journal and conference paper read, the most threat that’s been discussed by previous researcher are the malware which is 34% followed by security attack 30%. Loss or stolen device is 3rd main concern which is 19% and followed by data leakage 12%. Only 3% researcher talk about DDOS attack and 1% discuss on the unauthorized software and bandwidth problem.

Although most researchers discuss their opinion differently on the security threat, but most of the threat actually leads to data leakage. Malware is designed to retrieve information on the user computer and send it to the malware creator. This leads to company information being leaked. Security attack such as phishing, pharming, spoofing is designed to exploit people and steal confidential and sensitive information which also lead to data leakage. When the device was stolen or loss, the organization actually does not care about the device because the device belongs to the employee, but what they worry is the device that contains company sensitive data that will be expose to data leakage. Hence, it can be concluded that the major threat in BYOD is data leakage and this is the issue that need to be looked into by the organization before implementing BYOD.

In order to detect and prevent data leakage, there are a few techniques that can be used. The first technique is by using a watermark to develop guilty agent. This works by modifying the data. The process of data modifying is called perturbation [3]. The disadvantages of using the watermarking technique are by doing perturbation it actually makes the original data less sensitive. The watermark also can sometimes be destroyed if the recipients are malicious. Another technique to prevent data leakage is using data allocation strategies for improving probability of identifying guilt agent. The private key is usually used for each set of distributed data [10]. In the era of cloud computing, researchers had started to look into data leakage detection using the cloud. This technique used allocation strategies while adding a fake record in the dataset, which the probability of identifying leakage in the system can be improved [11]. In BYOD, data leakage is controlled in organization by implementing a framework and security control.

There are a few available security controls to protect BYOD environment from data leakage like desktop application virtualization, Network access control, Mobile device management, Mobile application management, Access control mechanism and identity access management. Desktop application virtualization uses techniques such as heavy-duty virtual machine [12], simplified lightweight virtual box [12], and VMware Horizon Mobile [13]. The limitation of those techniques is not all mobile devices meet the system requirement to run virtual application and it depends on the network connection to access the resources. A technique like CISCO Network BYOD Solution [14] and MERU Network BYOD Solution [15] used network access control. The limitation of those types of controls is the compatibility and support issues of various devices with different OS and also depending on network connection.

Mobile device management (MDM) is one of the security controls that are widely used. Existing techniques that available are VMware (AirWatch), MobileIron, and FiberLink [16], AmTel MDM, FancyFon [5] and Maas360, Zenprise MobileManager [12]. However, this type of security control does not separate personal and corporate space. It also has a problem in handling multiple user roles. User also loses flexibility because they need to install the policy application on their device. Beside MDM there is also a Mobile application management technique like VMware (AirWatch) [16] but still it can’t support different device platform. [17] used access control mechanism for his T-Dominance technique, but it depends on the network connection and required high-speed bandwidth. The most common security controls being used in BYOD environment are identity and access management. This type of control involves single factor authentication, two-factor authentication and also multi factor authentication. It depends on user involvement to secure the environment. Most of the researcher uses a combination of technique because every technique has its own limitation.

Even with the variety of security control in BYOD, the cases of data leakage are still happening. This is because of focusing in a way of preventing it without looking at the root cause of the data leakage problem, which is the weak authentication technology and unsecure record keeping technique.

2.2. Blockchain

Blockchain is a cryptographic technology that record all user transactions in a digital ledger that distributed across the network [18]. Blockchain platform is not dependent to any individual entity because the ledger is shared in a decentralized way. It prevents occurrence of human errors in which make it reliable. The record can be access from anywhere and the confidentiality of the data is maintained by encryption and hashing method [19]. The use of cryptography prevents unauthorized access to the network and ensure only legitimate user are allowed to participate. When the blockchain technology is being used, the new block will be added to the previous blocks and complex mathematical puzzles need to be solved which called proof-of-work. This complex puzzle makes blockchain secure and highly tamper-resistant.

Blockchain was introduced by pseudonym Satashi Nakamto as the underlying technology behind bitcoin. Bitcoin is an electronic cash system or cryptocurrency that used peer-to-peer concept in maintaining all transactions in a distributed ledger [7]. The ledger will be available to all the peers in the network to maintain the security of the system. Blockchain can be categorized into three type which is the public blockchain where everybody can join the network, a consortium blockchain which combine public and private network and a private blockchain where the member of the network only limit to certain group or organization.

The blockchain technology nowadays hasn’t only been used in currency but towards widely aspect of life such as smart contract, record keeping, ID systems, cloud storage and many more [20]. One example used of blockchain is crowdfunding where the idea is that peer-to-peer fundraising models can supplant the need to have to go thru a third party. Blockchain has also been used in a smart property aspect where it can register any form of hard asset and intangible assets inventory and exchange. Blockchain-encoded property becomes smart property that is transactable via smart contracts.

One of the first noncurrency uses of blockchain technology is Namecoin which is an alternative DNS registration. Namecoin is a decentralize DNS that is not control of any government or cooperation and it is possible for anyone worldwide to register their own DNS. For digital identity registration, OneName and BitID come out with decentralize digital identity verification system using blockchain technology to speed up the verification process. Blockchain also have been used in voting system where the vote is done and stored in decentralize environment which make the result tempered-free and secure.

Blockchain technology also been developed on supply chain, power and food/agriculture. These areas are arguably strong fits for blockchain. These industrial use cases are believed to deliver real ROI at an early stage of blockchain development [21]. It will help to control supply and demand of product because the chain of each product can be traced and recorded. Nowadays, people are talking about Internet of things and blockchain can be used as smart contracts that facilitate and enforce the negotiation of a contract in the IoT [22].

In the public sector, governments in Asia and Europe have started to consolidate and linking their records. Estonia had been using blockchain-like technologies to secure health records, while Georgia's National Agency of Public Registry recently moved its land registry onto the blockchain. China is questioning on the cryptocurrency but are very positive on the use of blockchain in another sector. Sweden is in the midst of testing a blockchain-based land registry while Dubai plans to run its entire government using blockchain technology by 2020. Japan is looking at cryptocurrency to use it as their own digital currency while Venezuela recently launched a cryptocurrency in an attempt to circumvent financial blockades. By using a blockchain, governments can address the dual challenges of trust and transparency, and the need for data protection and privacy [23].

Blockchain technology could simplify the management of trusted information, making it easier for government agencies to access and use critical public-sector data while maintaining the security of this information. Based on a survey by [24] of more than 200 regulators in 16 countries, addressing a security concern are the 2nd reason company are shifting to blockchain as Figure 1.

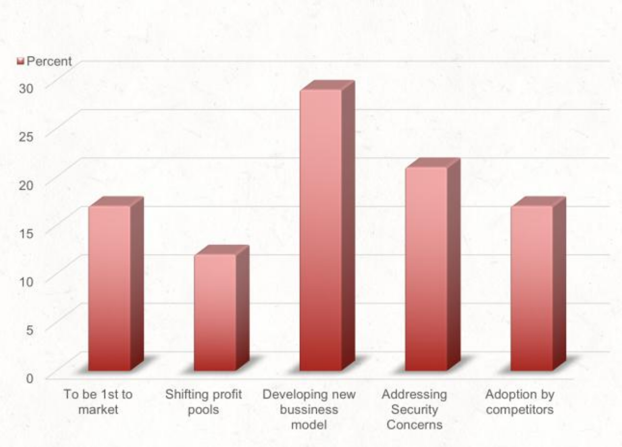

Fig. 1: Factor influence blockchain (IBM, 2017)

The blockchain technology main characteristic are decentralized, persistency, anonymity and auditability that make it great for cost saving and improve efficiency [25]. Storing data in a centralize server like traditional way are not secure anymore. It's prone to hacking and data leakage. What's required is an environment in which data can easily be shared across systems, but in which individuals and organizations can take back ownership of their data and control the flow of personal information—who sees it, what they see, and when. Blockchain is the answer to such a scenario. Each person or organization would have all relevant data about them stored in a dedicated ledger within an encrypted blockchain database. They could use public keys to selectively share information relating to a particular service transaction with agencies. Or they could issue private keys to agencies for one-time "write" access to their data.

There are a few disadvantages of blockchain which is scalability and privacy leakage. Since each node has to store all transaction in order to validate, it will need a high processing power and a huge storage in each node. It will also require a high speed bandwidth to run the blockchain. In order to minimize this issues a few effort has been done by [26] where he came out with the mini blockchain scheme where old transaction and record are removed left only the current one. Versum technique was introduced by [27]where lightweight client being used to outsource large and frequently changing data structure. This will make sure the output is correct by comparing to multiple server. In 2016 [28] Introduce a Bitcoin NG (Next generation) where he solves the scalability issue with a technology that design to scale the block by dividing it into two part which is key block and micro block. The second disadvantage is the privacy issues where it is possible to track user identity from the ledger even though user use their public key and private key for doing transaction and they supposed to be anonymous. In 2018, [29] introduce a Coinparty where he combines the advantage of centralize and decentralize solution to solve the privacy issue.

The use of blockchain ledgers would reduce the risk of data leakage through strong encryption and a tamperproof audit trail. However, the use of blockchain technology in BYOD environment has not been explored further.

3. Architecture Overview

This section discusses an overview of the propose BYOD Trust Model Architecture. As illustrated in Figure 2, the input of this research is the current existing (BYOD) security problem. The main problem with BYOD is on the data leakage issue. There are a lot of way data can be leaked if the organization implements BYOD. This research will look into the data leakage through unauthorized access and malware infection. For this issue, this research will propose an authentication user trust model and agentless device trust model including location detection. Data leakage can also happen through insider which is the authorize access. For this we proposed a record storing technique using blockchain, including the authentication record. It is also difficult to collect evidence if data leakage happens for further investigation. To tackle this issue, this research proposes an evidence collection using digital ledger in blockchain.

The output of this research will be a comprehensive BYOD trust model architecture. This architecture will use blockchain technology to secure the authentication and record keeping technique. The architecture will be divided into 3 phases which is an Authentication Trust Model that comprise of user and device authentication with location detection capability. Second phase is the Secure Record Keeping where all updating will go through the blockchain process. The last phase is the Evidence Collection Technique where a digital ledger from the block chain will be used to record all user and device activity.

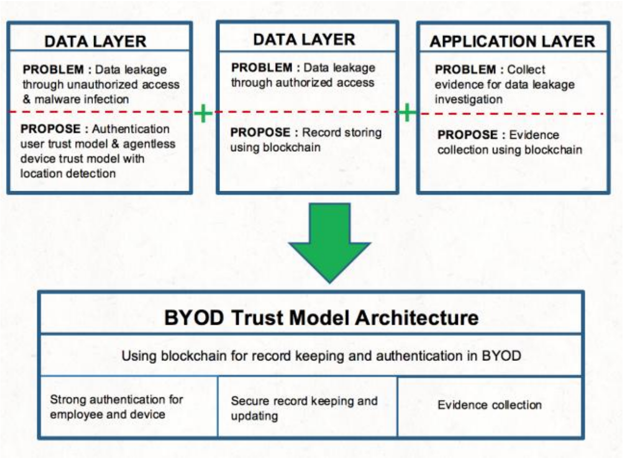
DATA LAYER
PROBLEM : Data leakage through unauthorized access & malware infection
PROPOSE : Authentication user trust model & agentless device trust model with location detection
DATA LAYER
PROBLEM : Data leakage through authorized access
PROPOSE : Record storing using blockchain
APPLICATION LAYER
PROBLEM : Collect evidence for data leakage investigation
PROPOSE : Evidence collection using blockchain
BYOD Trust Model Architecture
Using blockchain for record keeping and authentication in BYOD
Strong authentication for employee and device
Secure record keeping and updating
Evidence collection

Fig. 2: Research Input and Output

The overall BYOD trust model architecture is divided into 4 main parts as shown in Figure 3. The first part is a user authentication process. It will use multifactor authentication where the user needs to key in their ID and password. The authentication process then will go through the blockchain process where a private key and public key will be assigned to the user. Blockchain used asymmetric cryptography mechanism to authenticate transaction that's why each user must own a private and public key [25]. Data on employee Private key is not kept in the database but only stored in the blockchain. If user lost their private key, they need to request from the system admin for a new key. For public key, users will also get it during the registration process. This key will act as user identification in the blockchain. The key will be kept in the authentication database. Once authenticate, users will allow to access organization record.

The second part is the device authentication process where the device will go through two phases. The first phase is where the malware database server will do offload scanning and scan if the device is clean. The malware database consists of an updates malware list and malware calculation detection. If the device is clean, the device will go through the second phase of the authentication which is location detection. Here the network will detect if the device is in the organization's network, it will grant access, but if it is out of range, a verification code will be sent to the user through email and user need to key in the verification code as prove the device are used by legitimate users. This authentication is agentless where it will do off load scanning through the network without the user needing to install anything to the device.

The third part is the record keeping process. All records will be kept in the organization database, including employee personal data and authentication. However, this record will be linked to blockchain where there are kept in cryptography format and can only be updated with the appropriate authentication. Every change made to the document will be notified by the owner and everyone in the chain. Blockchain is secure because any changes done by an unauthorized user, a notification will be sent to the owner [20].

The last part of the architecture is the evidence collection. Since authentication and record keeping will go the through the blockchain process, all user activity will be recorded in the digital ledger. This digital ledger is tempered free and can be viewed by everyone one the loop. This can be a perfect evidence for investigation if data leakage happens in the organization.

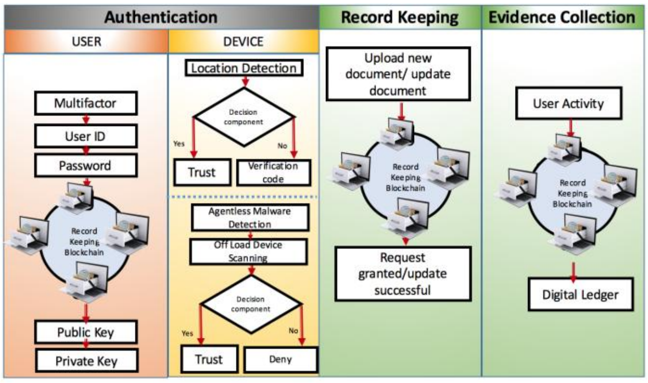

Fig. 3: BYOD Trust Model Architecture

The blockchain detail architecture are shown in Figure 4. Blockchain will keep authentication information and record information in the cryptography format. We divided the process into three parts as below

3.1. For New User

(1) IT admin will register new user & the device after passes the authentication process. (2) Etherium client will create a new block in the existing blockchain and add a new smart contract. Etherium client will post the new user information to the blockchain and link the user with the smart contract. (3) Miner will do the mining and return with the public and private key for the new user. The block record will be kept in cryptographic format. (4) Etherium client will update the user smart contract with the private and public key. (5) Notification will be sent to the user to acknowledge they already authenticate and to inform their private and public key. (6) The notification will be updated in the smart contract. (7) User database will be updated with the new user record and their public key only. The private key will not be kept in the database. (8) Database gateway will update Etherium client on the new changes in the authentication database.

3.2. For Existing User to Upload New Record

(1) After user and device successful authentication, the user will upload a new document. He/she will decide the access control to the document weather need to key in public key only or both public and private key. (2) Etherium client will create a new block in the existing blockchain and add a new smart contract. Etherium client will post the new user record to the blockchain and linked the record with the smart contract. The new block will also be link to user existing block. (3) Miner will do the mining and give identification to the record and set the access control (public key only or both private and public keys). (4) Etherium client will update record smart contract with access control requirement. (5) Notification will be sent to the user to confirm the adding record and required the user private key. (6) Notification and private key status will be updated in the record smart contract. (7) The record will be updated in the record database. (8) Database gateway will update Etherium client on the new changes in the database.

3.3. Existing User Accessing Existing Record

(1) After user and device successful authentication, the user will choose a record he/she want to view/update. Here he/she need to key in public/private key base on the record requirement. (2) Etherium client will check on the existing block and all related smart contracts to the record. (3) Miner will do the mining and check access control with all the smart contract related to the requested block. It will also check on the user (requester) public/private key in the user smart contract. (4) Etherium client will update record smart contract with access control requirement and all the block related to the request. (5) Notification will be sent to the user to reject or accept the request. (6) Notification and private key status will be updated in the record smart contract. (7) User (Requester) will be granted access to view/update the record base on permission give on the record database. (8) Database gateway will update Etherium client on the new changes in the database.

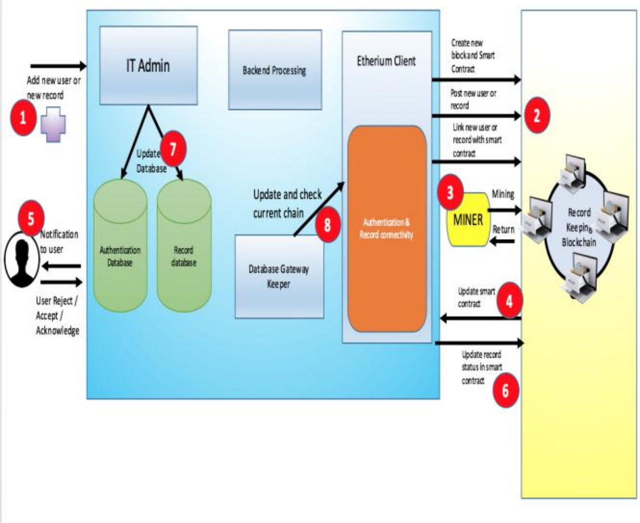
Add new user or new record
1
IT Admin
Backend Processing
Etherium Client
Update Database
7
Authentication Database
Record database
Update and check current chain
8
Database Gateway Keeper
Authentication & Record connectivity
5
Notification to user
User Reject / Accept / Acknowledge
Create new block and Smart Contract
Post new user or record
2
Link new user or record with smart contract
3
MINER
Mining
Return
Record Keeping Blockchain
Update smart contract
4
Update record status in smart contract
6

Fig. 4: Blockchain Architecture

The function of the backend library is to export Application Programming Interface (API) function and communicate with blockchain. Backend library will also interact with a user interface where users need to login to the system and interact with Etherium client. Etherium client is the heart of the blockchain. It will handle tasks such as connect all nodes in the chain, encode/decode every transaction and decide only node that meet full requirement can join the chain. Etherium client also will keep verified local copy of every transaction in the blockchain.

The database in the figure 4 is existing organization database where they kept employee personal information, authentication data and also sensitive documents. This database will be linked to the blockchain using database gatekeeper. The gatekeeper will listen to query request by the user from the chain. The gatekeeper will confirm the identity of the requester from the blockchain authentication process. If the request is coming from a valid source, it will notify the database to return a result to the requester. IT Admin in figure 4 is actually a system that stores all documents in the database and will update the database when required.

4. Future Direction

As discussed above are the general overviews of our BYOD Trust Model Architecture. Next step we are going to start developing the system and divided it into 3 phases which is the Authentication, Record Keeping and Evidence collection. We will be using a virtual machine to create the blockchain environment and used Debian as main operating system. For programming language, we will be using Etherium combining with Java and Python. For Etherium client, we will be using PyEthereum and PyethApp Client. For the user interface, we will be using a python micro framework (FLASK). For storing the record in the blockchain, we will modify a technique introduce by [22] which is Sapphire where it uses data analytics for large-scale blockchain-based in the Internet of Things and a MedRec technique introduce by [30].

Although we secure the system with multifactor authentication combining with blockchain cryptography, the major challenge that needs to be looked into is the user. If the user public and private key are lost or stolen, the blockchain security can be compromised, especially in BYOD where the user tends to store their keys in their own device. It is a challenge that needs to be discussed further for future extension.

5. Conclusion

This paper discusses about the use of blockchain to minimize data leakage issues in Bring Your Own Device (BYOD) technology. As it exists now, data leakage is the main security issues facing by organization that implement BYOD. Using blockchain with additional security features will help to detect data leakage cases. The use of user authentication combining with device trust model will help to solve data leakage because of loss or stolen device, malware and prevent unauthorized person to access the information. Record keeping will help organization to secure their sensitive data and prevent authorized user to leak the data. Digital ledger in blockchain will provide evidence of every user transaction that can be used as evidence when data leakage occurs. It's also can be used by digital forensic team to find evidence of security attack. The blockchain technology that comes with cryptography will allow the organization to protect their sensitive data and prevent from leaking even when an employee brings his or her own device to the organization. The future research of this project will explore implementation of the methods and start developing the algorithm for the whole BYOD Trust Model in minimizing the data leakage.

Acknowledgement

We acknowledge that this research received support from the GP-IPS Grant GP-IPS/2018/9644000 awarded by Universiti Putra Malaysia to the Faculty of Science Computer and Information Technology.

References

[1] N. Leavitt, "Security Requires a New Approach," pp. 16–19, 2017.

[2] J. Ni, X. Lin, K. Zhang, Y. Yu, and X. S. Shen, "Device-invisible two-factor authenticated key agreement protocol for BYOD," *2016 IEEE/CIC Int. Conf. Commun. China, ICCC 2016*, 2016.

[3] A. Mishra and K. Jani, "Comparative study on bring your own technology [BYOT]: Applications & security," *Int. Conf. Electr. Electron. Signals, Commun. Optim. EESCO 2015*, 2015.

[4] G. Thomson, "BYOD: Enabling the chaos," *Network Security*, vol. 2012, no. 2, Elsevier Ltd, pp. 5–8, 2012.

[5] V. Gupta, D. Sangroha, and L. Dhiman, "An Approach to Implement Bring Your Own Device (BYOD) Securely," *Int. J. Eng. Innov. Res.*, vol. 2, no. 2, pp. 154–156, 2013.

[6] P. Mamoshina *et al.*, "Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare," *Oncotarget*, vol. 9, no. 5, pp. 5665–5690, 2015.

[7] W. Ying, S. Jia, and W. Du, "Digital enablement of blockchain: Evidence from HNA group," *Int. J. Inf. Manage.*, vol. 39, no. October 2017, pp. 1–4, 2018.

[8] M. Swan, *Blockchain BLUEPRINT FOR A NEW ECONOMY*, First Edit. O'Reilly Media, Inc, 2015.

[9] M. Olalere, M. T. Abdullah, R. Mahmod, and A. Abdullah, "Bring Your Own Device: Security Challenges and A theoretical Framework for Two-Factor Authentication," *Int. J. Comput. Networks Commun. Secur.*, vol. 4, no. 1, pp. 21–32, 2016.

[10] M. M. Singh *et al.*, "SECURITY ATTACKS TAXONOMY ON BRING YOUR OWN DEVICES (BYOD)," vol. 4, no. 5, pp. 1–17, 2014.

[11] C. Bhatt and P. D. Kapgate, "Data Leakage Detection Using GSM," vol. 3, no. 6, pp. 873–877, 2014.

[12] Y. Wang, J. Wei, and K. Vangury, "Bring Your Own Device Security Issues and Challenges," in *The 11th Annual IEEE CCNC-Mobile Device, Platform and Communication Bring*, 2014, pp. 80–85.

[13] T. Vmware and M. Secure, "Mobile Secure Workplace – White Paper: VMware, Inc.," 2013.

[14] J. Bradley, J. Loucks, J. Macaulay, R. Medcalf, and L. Buckalew, "BYOD: A Global Perspective Harnessing Employee-Led Innovation Executive Summary Horizons Cisco IBSG Introduction: BYOD Has Gone Global," 2012.

[15] M. Networks, "BYOD Best Practices," 2012.

[16] C.-C. Chang, W. Cheng-Chieh, and S.-C. Chen, "The Influence of Bring Your Own Device on the Psychological Climate at Workplace," in *Proceedings of the Sixteenth International Conference on Electronic Commerce - ICEC '14*, 2014, pp. 9–16.

[17] W. Peng, F. Li, K. J. Han, X. Zou, and J. Wu, "T-dominance: Prioritized defense deployment for BYOD security," in *2013 IEEE Conference on Communications and Network Security, CNS 2013*, 2013.

[18] H. M. Gazali, R. Hassan, R. M. Nor, and H. M. M. Rahman, "Re-inventing PTPTN Study Loan With Blockchain and Smart Contracts," 2017.

[19] Archa, B. Alangot, and K. Achuthan, "Trace and track: Enhanced pharma supply chain infrastructure to prevent fraud," in *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, 2018.

[20] I. Zikratov, A. Kuzmin, V. Akimenko, V. Niculichev, and L. Yalansky, "Ensuring data integrity using blockchain technology," *Conf. Open Innov. Assoc. Fruct*, vol. 2017–April, pp. 534–539, 2017.

[21] N. Kshetri, "Blockchain ' s roles in meeting key supply chain management objectives," *Int. J. Inf. Manage.*, vol. 39, no. December 2017, pp. 80–89, 2018.

[22] Q. Xu, K. Mi, M. Aung, Y. Zhu, and K. L. Yong, "A Blockchain-Based Storage System for Data Analytics in the Internet of Things," *Springer Int. Publ. AG 2018*, pp. 119–138, 2018.

[23] R. Wattenhofer, *The Science Of the Blockchain*. Inverted Forest

Publishing, 2016.

[24] F. Kosmatos, "IBM Institute of Business Value: Rethinking Enterprises, Ecosystems and Economies with Blockchains.," *IBM Institute for Business Value*, no. March, 2017.

[25] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology : Architecture , Consensus , and Future Trends," 2017.

[26] J. D. Bruce, "The Mini-Blockchain Scheme," 2014.

[27] M. Csail, M. F. Kaashoek, and N. Zeldovich, "VerSum: Verifiable Computations over Large Public Logs Jelle van den Hooff," 2014.

[28] I. Eyal, A. E. Gencer, E. G. Sirer, and R. van Renesse, "Bitcoin-NG: A Scalable Blockchain Protocol," 2015.

[29] J. H. Ziegeldorf, R. Matzutt, M. Henze, F. Grossmann, and K. Wehrle, "Secure and anonymous decentralized Bitcoin mixing," *Futur. Gener. Comput. Syst.*, vol. 80, pp. 448–466, 2018.

[30] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," *Proc. - 2016 2nd Int. Conf. Open Big Data, OBD 2016*, pp. 25–30, 2016.