International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 05 | May 2019 www.irjet.net p-ISSN: 2395-0072

# SECURING THE TRANSFER OF CONFIDENTIAL DATA IN FISCAL DEVICES USING BLOCKCHAIN

**BOBBY K SIMON, ANJANA P NAIR**

*[1]BOBBY K SIMON M.Tech Computer Science & Engineering. Sree Buddha College of Engineering, Ayathil, Elavumthitta, Pathanamthitta , Kerala, India.*
*[2] Ms. ANJANA P NAIR Assistant Professor Computer Science & Engineering. Sree Buddha College of Engineering, Ayathil, Elavumthitta, Pathanamthitta, Kerala, India*

---

**Abstract** *The data transfer in fiscal device terminals are utilized as inward or outside specialized GPRS gadgets, sending charge related data from financial money registers and monetary printers to an expense organization server, so cyber security is of fundamental significance. With a huge amount of personal data in big data era, fiscal devices are at high risks associated with potential disclosure of privacy data. In this paper, a trustworthy method is proposed during transaction phase, which helps to protect user's data. The method proposed is AES 256 and it also helps to encrypt the user's personal data with 256 bit key. Since the amount of data is very large the concept of block chain is used. It helps in reducing the storage space and also protects the stored data with the help of SHA. For processing this bulk of data Hash function is being used. This paper also implements security of stored data for each tax payer with the help of block chain.*

***Key Words***: **AES, SHA, MLP, IT, IOT, PT, BLOCKCHAIN**

## 1. INTRODUCTION

Data security refers to the method of protective knowledge from unauthorized access and knowledge corruption throughout its lifecycle. Data security includes encryption, tokenization, and key management practices that defend knowledge across all applications and platforms. Organizations round the globe area unit finance heavily in info technology (IT) cyber defense capabilities to shield their important assets. Whether associate degree enterprise has to defend a complete, intellectual capital, and customer information or provide controls for critical infrastructure, the means for incident detection and response to protecting organizational interests have 3 common elements: individuals, processes, and technology. Software-based security solutions inscribe the info to shield it from thieving. However, a worm or a hacker might corrupt the info so as to create it irrecoverable, making the system unusable. Hardware-based security solutions will forestall browse and write access to knowledge and thence provide terribly sturdy protection against change of state and unauthorized access. Data transfer is that the method of exploitation computing techniques and technologies to transmit or transfer electronic or analog knowledge from one laptop node to a different. Data is transferred within the type of bits and bytes over a digital or analog medium, and the process enables digital or analog communications and its movement between devices. Fiscal memory devices area unit electronic devices used for management of a country's tax revenues. Currently they're wide employed in several countries round the world, as well as Russia, Bulgaria, Serbia, Romania, Republic of Macedonia, Albania, Poland, Moldova, etc., commercial enterprise memory itself may be a kind of memory that's certified by acceptable government body. This Encrypted module is usually in the form of an IC on the Electronic circuit. In the data transferring many threats are in the process, so we use AES or Advanced Encryption Standard is a cipher, i.e., a method for encrypting and decrypting information. Whenever you transmit files over secure file transfer protocols like HTTPS, FTPS or SFTP, there's a good chance your data will be encrypted by some flavour of AES - either AES 256, 192, or 128.1.1

### 1.1 Objective

This proposed framework has significant applications in a variety of security methods. For instance, consider a huge amount of confidential data transferring to online system for business purpose. The individual data transferring to online in a way that it does not hack the data on that transformation for using AES 256 bit key but the bulk of data transfer are hacked of these transaction, it was affected on banking sector. In this case the banks and other tax departments are detecting the attacker and the data is getting safe due to the transactions using block-chain method. In Oder to do so, if first users are one of the taxpayer's personal data to get encrypted using AES 256 from that the huge confidential data of one branch of a bank to get transfer and store using block-chain method (block models) Finally, from a big security perspective, we use and blockchain technology helps to make online data transmission secure by eliminating middlemen and singular control. Because the blockchain is completely decentralized, there is no single source controlling it. If a block is added which attempts to cheat the system, it will look markedly different from the others. Because the blockchain requires the consensus of all users, the malicious version of the blockchain is

instantly disposed of. While many of us associate the blockchain concept with crypto currencies and data transferring this emerging technology can be used to record virtually anything of tangible value. It's not simply to attack the preserve of digital finance, as many may have initially thought.

## 2. METHODOLOGY

The development of this project is done in Microsoft Visual Studio.Net, which is an integrated development environment (IDE) from Microsoft.C# programs run on the .NET Framework, an integral component of Windows that includes a virtual execution system called the common language runtime (CLR) and a unified set of class libraries.ASP.NET is a web development platform, which provides a programming model, a comprehensive software infrastructure and various services required to build up robust web applications for PC as well as mobile devices. The project is proposed to be developed in ASP.Net as front end and SQL Server 2008 R2 as back end which develop to help powerful software. With the help of these tools and techniques, this project can be implemented.

### 2.1 Existing System

GPRS terminals are used as internal or external communication devices, sending tax related information from fiscal cash registers and fiscal printers to a tax administration server. Many IoT devices exchanged completely unencrypted information with servers. Using AES 128 bit is used for processing the data transfer. The tax administration server communicates with the existing fiscal device using plaintext (PT), i.e. non-encrypted data, passing through the existing GPRS terminal and telecommunication operator's nodes including the transaction (journal) memory, with the external optional computer device.

#### 2.1.1 Disadvantages

- Existing method provides less security for data transfer.
- If the data transfer uses symmetric Algorithm and if the key is leaked to the users, then the data will be visible to third party and the confidential data will be masquerade.
- The difficulties and costs of implementing encryption on technically limited IoT devices is well known problem.
- Large storage space is required for the huge data.

### 2.2 Proposed System

The main focus relays on secure data transfer during the transaction. The tax payer's user data are securely saved using AES-256 bit key. These data can be viewed only by tax payer and the authority. Also, the data will be saved in data server by encryption Algorithm. Along with this, even if the respective authority wishes to see the taxpayer personal information, then they have to decrypt the data with their authority ID and password. When the amount of data is as huge as Data warehouse, the respective authority will transfer the data to their headquarters with the help of block-chain. This is mainly done for the security purpose during the data transfer. Those data will also be stored and saved in this block-chaining as blocks of data. When an attacker performs his job, the data will not be modified or deleted neither the tax person's personal information will be gained, it will be integrated. Along with this the tax payer will be noticed by an SMS and Email that their account is being hacked. This project is also designed for user-friendly purpose.

## 3. SYSTEM ARCHITECTURE

- This software is being designed for the Tax Department to ensure about the tax payer citizen.
- It is also designed by 3 modules, which includes tax payer, Admin and Attacker.
- In tax payer each user can register with their Tax number, shop license, email Id, machine Id and mobile number. With this and One-time password (OTP) will be generated. Then the tax payer can login with their Tax payer Id and password.
- For the Tax payment, the accessed Tax payers can view 3 lists as Tax view, Tax payer list and Defaulters list.
- In Tax view, the authority will display the amount needed to be payed by the particular user and the period of time (duration), it should be payed.
- To the settle the amount, the tax payer can pay the money through online transaction with their respective information. In this the transaction is also secured using OTP during the money transfer. Then a POP can be generated to show that our transaction was successful.
- These data will be automatically encrypted using AES-256 bit Algorithm. The data will be tightly secured in the data server. Even the authority also cannot read or modify the data. These encrypted data will be in binary bit form.
- In Tax payer list the users can view, whether their payment is processed or not within the duration time.

- Defaulters list is used to display those users who has not payed their Tax.
- In the second module, each Authority should register their official details. The Admin is in charge of payment approval, detail report of tax payer, payed user and not payed users can be viewed. The stored data and transferred can also be viewed by them. They can also identify the attack performed by the attackers and the machine used to perform this attack, along with their IP address.

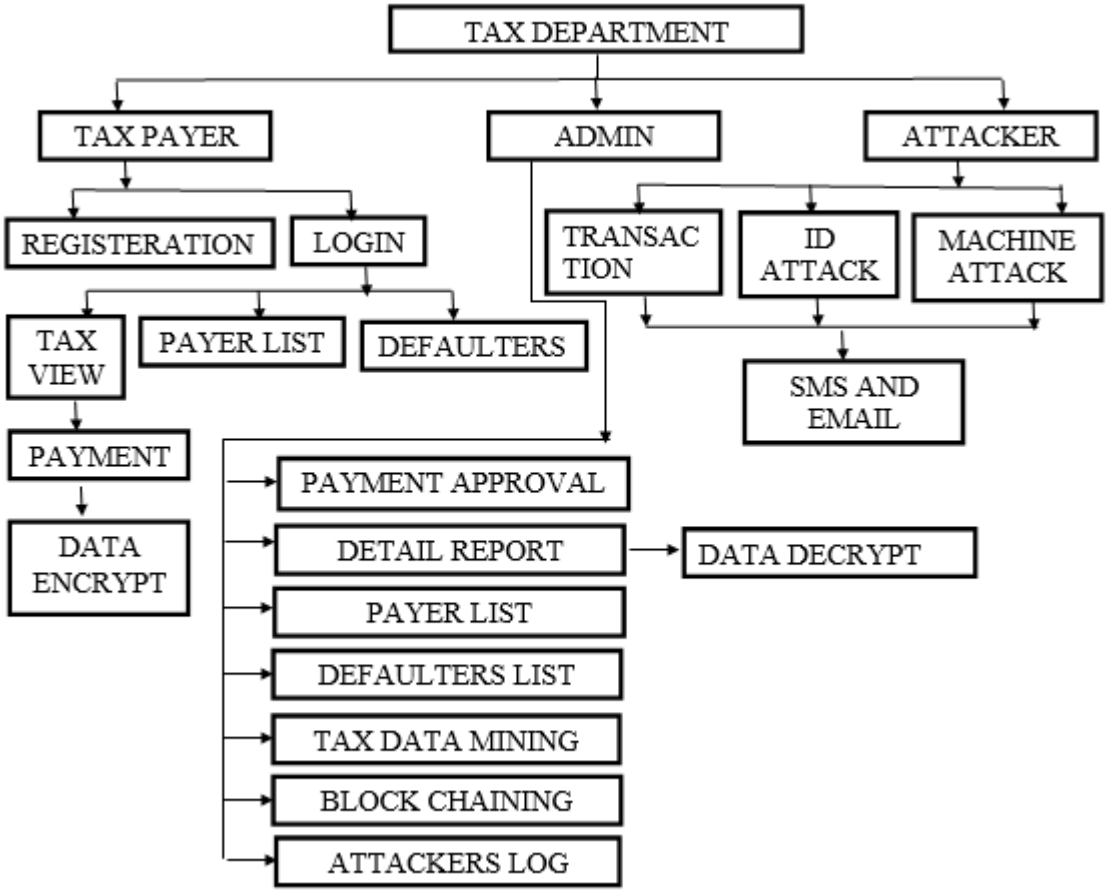


**Fig 3.1: System Architecture**

- Payment Approval is used to ensure the payment list of users and to mention amount needed to be payed by each payer.
- Tax payers list and Default list is to verify the payed user and non-pay users.
- The detailed report will be viewed by the authority, but to view their personal information they have to login again with their authority id and password for more security purpose.
- Then the encrypted binary data will be decrypted to a readable form and displayed to the respective authority.
- Data analysis is used to store data, and to check the accuracy of data along with Recall and precision. To convert this data to ARFF form we use WEKA tool and apply MLP software, and precision, recall and accuracy of data will be generated.
- Block chaining is used for data securing during confidential data transaction. Here the authority can choose the method needed to transfer their data for data security.
- In case of SHA-1 we use MD5 Algorithm to transfer the stored data. In case of SHA-2 we use SHA-256 Algorithm to transfer the data, in case of SHA-3 we use SHA-384 Algorithm for transferring the data. In case of SHA-4 we use SHA-512 Algorithm for processing data.
- To produce block chaining, we use previous Hash function and chosen SHA Algorithm for the block data and a java script will be shown.

- The Tax authority can view the number of transaction and the time used to process this data along with the storage space required for the particular block data.
- Attacking log is used for the admin, to view and analyze the attack whether it is a transaction attack or machine attack or if any data being modified.
- A graph is used to display the attack analysis and the number of times attack has occurred will be shown in a grid.
- If an attack is occurred in this software, we can analyze and track the attacker IP address. With this we can verify that whether our data is being modified or deleted.
- In case of Attacker, he can perform attack during transaction. The attack can be performed through a machine Id or can also perform attack in Tax payer personal data.
- To make this project more efficient for the users, the user will get notification through SMS or email if their account is being hacked.

## 4. ALGORITHMS

### 4.1 AES-256 Encryption Algorithm

The algorithm is implemented as given below

Step 1: when users details are submitted to the admin, each individual users data are encrypted.

Step 2: Keys are encrypted by AESexample.cs (algorithm used in the software) i.e., the object used for data encryption. “Sytem.security. cryptography framework” is used to encrypt the data.

Step 3: To encrypt, each users tax payer-Id are encrypted by using a session and details will be encrypted.

Step 4: During each transaction a random trans key will be generated and stored in table.

Step 5: With this 2 keys will be generated i.e., key 1- secret key, and key 2- initialization vector(IV) form transaction keys to generate byte.

Step 6: Next using this byte each transaction details will be encrypted of each user.

Step 7: These encrypted data’s will be store as var-binary in database.

Step 8: During payment for further verification we ask users tax Id and password. For generating OTP, in algorithm we have provided the number range of 10000 – 200000 and for each user a random number will be generated.

Step 9: And a pop message will be generated as a java script that means payment is successfully completed.

Similarly AES-256 decryption is also performed.

### 4.2 Block Chain Method

Originally a blockchain is a growing list of records called blocks, which are linked using cryptography. Each block contains a cryptographic hash function with a previous continues block of a timestamp and the transaction data. The blockchain is designed as; a blockchain is non-resistant to modification of the data. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way. Blockchain is considered a type of payment rail. Private Blockchain has been proposed for business use. Sources such as Computerworld called the marketing of such blockchain without a proper security model "snake chain”. The method is implemented as given below.

Step 1: After the calculation of precision, recall and accuracy value, the online transferring data are then used for blockchain method.

Step 2: In this database, when there are huge bulks of data for taxpayers, the details are Taxpayer ID, Tax amount, Date, Bank, PIN, Account number, Card number, Machine ID.

Step 3: Incase if the stored details of any data’s are accessed by an attacker or if they track the AES key then the data can be updated or changed. Then all the confidential data will be hacked.

Step 4: So, in this critic’s, the authority can create class name as block. In this block they assign an object. For that authority can apply SHA method in the blockchain technology.

Step 5: Used for SHA method. In case of SHA-1 MD5 Algorithm is used tto stored data. In case of SHA-2, SHA-256 Algorithm is used to secure the data, in case of SHA-3, SHA-384 Algorithm is used. In case of SHA-4, SHA-512 Algorithm is used for processing data.

Step 6: If the blockchain is applied to the framework, but in this case the data is of live transaction information. The transaction data will get encrypted for a secret password by using the hashing technique. This is used to make our data secure during storage.

Step 7: The stored block chain details include the secret password (calculated using hash function) and first taxpayer online transaction ID; these data will be secured in blockchain of each individual taxpayers.

Step 8: Similarly second transaction data will be secured. For securing the details of second transaction the result of first transaction is taken or hash function of some values and along with that second transaction ID, later all the data are of second online taxpayer.

Step 9: Then this process is continued, all the online transaction data can be secured in chain to chain or peer to peer process. These secured data will be in a block and stored in database as a blockchain.

Step 10: The securely stored data, if any of the attacker try to hack the taxpayer detail it could not be accessed.

Step 11: The reason is that if any of the attacker tries to update or hack the data then all the taxpayers transaction details will be removed in the database. i.e.; the technology of blockchain is used.

Step 12: The blockchain technology can be applied in the database for the highly confidential stored data, for the attacker not to access anyone's data.

### 4.3 Secure Hash Algorithm (SHA)

The Secure Hash Algorithms are a family of cryptographic hash functions published by the National Institute of Standards and Technology (NIST) as a U.S Federal Information Processing Standard (FIPS), including:

- SHA-1: A 160-bit hash function which resembles the earlier MD5 algorithm. This was designed by the National Security Agency (NSA) to be part of the Digital Signature Algorithm. Cryptographic weaknesses were discovered in SHA-1, and the standard was no longer approved for most cryptographic uses after 2010.
- SHA-2: A family of two similar hash functions, with different block sizes, known as SHA-256 and SHA-512. They differ in the word size; SHA-256 uses 32-bit words where SHA-512 uses 64-bit words. There are also truncated versions of each standard, known as SHA-224, SHA-384. These were also designed by the NSA.
- SHA-3: A hash function formerly called Keccak, chosen in 2012 after a public competition among non-NSA designers. It supports the same hash lengths as SHA-2, and its internal structure differs significantly from the rest of the SHA family. For this we use hash function SHA-384.
- SHA-4: For this we use SHA-512 where 64-bit words. Hash functions with different block sizes, known as SHA-512. There are also truncated versions of each standard, known as, SHA-512/224 and SHA-512/256. These were also designed by the NSA.

## 5. RESULT AND ANALYSIS

The purpose of system testing is to identify and detect the attacks occurred in the system. Testing is an important element of the software, quality and assurance represents the ultimate review of specification, design and coding. The increasing visibility of the software as a system element and the costs associated with a software failure are motivated forces for well planned testing. In this section, the calculated data analysis value is compared using MLP and accuracy, precision and recall values are calculated. Later shows how secured our software is? And how secured our data's will be? During blockchain technique transaction count is also calculated and storage space and time required for storing that particular data. And for result analysis graph representations are used to show the variations in the calculated values. Blockchain technique, in which during the data storage process it shows how much space is required to store the required data. And it also calculates the time required to process this technique. While this process gets preceded, the transaction of data is also counted along with this, i.e., blockchain technology also calculate the number of times data are securely stored.

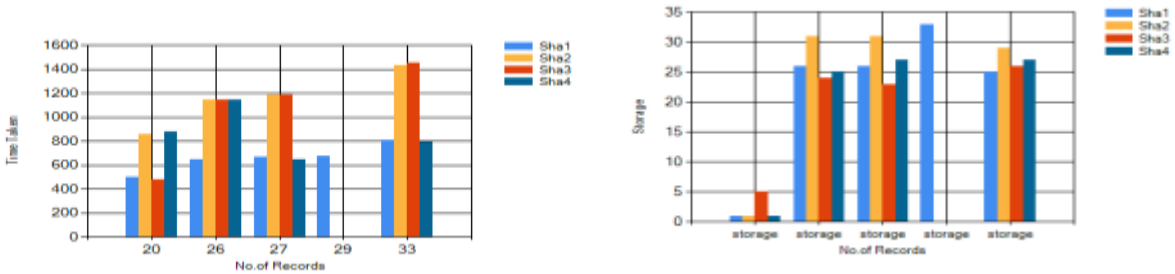


**Fig 5.1: Graph Showing Effiecency ,Storage and No of Records**

This diagram figure 5.1 Show the time taken during the records storage with all the SHA functions during the blockchain process and it also shows the space used for transaction data during blockchain and its space used to store these data. Figure 5.2 shows the bar chart diagram for data storage and time required to store all the data's. These different bar chart representations are used to show our blockchain efficiency and secure transaction data's can be stored in our database. Attack analysis is used for the possibilities or chances in which attack can occur during our online transaction, or using any random tax payerId, or with any machine Id's. Therefore with this Therefore with this graph it can be analyzed, that the high risk occurrence is in the online transaction details of the database system used for the tax payment.

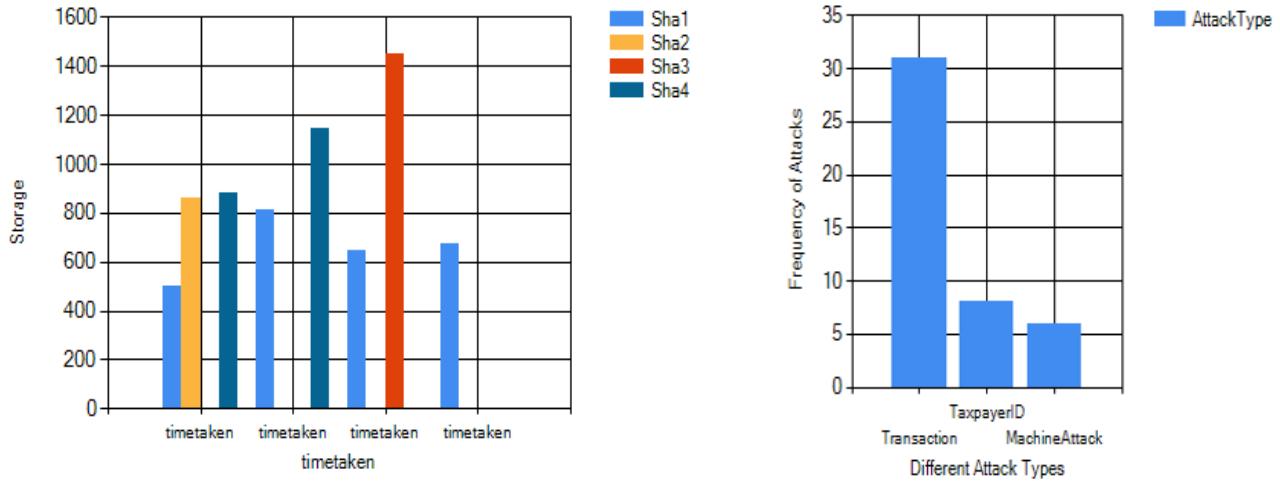


**Fig 5.2: Graph Showing Data Storage and Attack Analysis**

## 6. CONCLUSION

The proposed method shows that the software is highly secured for tax payment and also for sharing personal details. This software is developed for Tax department, and purpose include payment and to check the tax payment details and its validity. This can be divided in three ways such as tax payer (common users), Admin (tax authority) and Attacker. To secure the data transaction AES-256 bit encryption and decryption is performed. And huge confidential data's are stored using Blockchain technique with the help of hash functions such as SHA-1, SHA-2, SHA-3 and SHA-4. The attack phase is used to verify how well organized the software is. Even when an attack occurs it can be tracked using the attacker IP address. This is user friendly and is efficient to be used by all the citizens and this software also be used in any secure data transaction fields. For future enhancement, etheurium algorithm can be used for secure transactions.

## REFERENCES

[1] D. Kornack and P. Rakic, "Cell Proliferation without Neurogenesis in Adult Primate Neocortex," Science, vol. 294, Dec. 2001, pp. 2127-2130, doi:10.1126/science.1065467. [1] M. Prokin, D. Prokin, "First generation of turnover control devices," Proc. 19th Telecommunications forum (TELFOR), 2011, Belgrade, Serbia, pp. 888-891.

[2] M. Prokin, D. Prokin, "Improved fiscal devices without additional services," Proc. 5th Mediterranean Conference on Embedded Computing (MECO), 2016, Budva, Montenegro, pp. 273-276.

[3] "Common cyberattacks," Cert-UK, Internet: https://www.ncsc.gov.uk/ content/files/ protected_files/guidance_files/common_cyber_attacks_2016.pdf, Dec. 1, 2015 [Feb. 16, 2018]

[4] "Fostering the advancement of the Internet of Things," The Department of commerce, Internet policy task force & Digital economy leadership team, Washington DC, USA, Jan. 2017.

[5] J.A. Eisenach, C. Barfield, J.K. Glassman, M. Loyola, S. Tews, "An American strategy for cyberspace – Advancing freedom, security, and prosperity," American Enterprise Institute, June 2016.

[6] "Threats report," McAfee Labs, Intel Security, Aug. 2015.

[7] L. Constantin, "Armies of hacked IoT devices launch unprecedented DDoS attacks." Internet:https://www.pcworld.idg.com.au/article/607509/armies-hacked-iot-devices-launch-unprecedented-ddos-attacks/, Sep. 27, 2016 [Feb. 16, 2018]

[8] S. Ragan, "Here are the 61 passwords that powered the Mirao IoT botnet." Internet: https://www.csoonline.com/article/3126924/security/here-are-the-61-passwords-that powered-the-mirai-iot-botnet.html, Oct. 3, 2016 [Feb. 16, 2018]

[9] D. Storm, "Code in the wild to infect millions of IoT devices for crippling DDoS attacks." Internet: https://www.computerworld.com/article/3126864/security/code-in-the-wild-to-infect-millions-of-iotdevices-for-crippling-ddos-attacks.html, Oct. 3, 2016 [Feb. 16, 2018]

[10] E. Dresselhuys, "To predict the IoT future, it helps to look to the past." Internet: https://readwrite.com/2016/10/03/predict-iot-future-pl1/, Oct. 3, 2016 [Feb. 16, 2018]

[11] M. Ramsinghani, "How the 'insecurity of things' creates the next wave of security opportunities." Internet: https://techcrunch.com/2016/06/26/ how-the-insecurity-of-things-creates-the-next-wave-of-securityopportunities/, Jun. 26, 2016 [Feb. 16, 2018]

[12] Y.M.Pa Pa, S. Suzuki, K. Yoshioka, T. Matsumoto, T. Kasama, C. Rossow, "IoTPOT: A novel honeypot for revealing current IoT threats," Journal of Information Processing, vol. 24, no. 3, May 2016, pp. 522- 533.

[13] D. Coldewey, "This security camera was infected by malware 98seconds after it was plugged in." Internet: https://techcrunch.com/2016/ 11/18/this-security-camera-was-infected-by-malware-in-98-secondsafter-it-was-plugged-in/, Nov. 18, 2016 [Feb. 16, 2018]

[14] L. Tung, "Mozilla: The internet is unhealthy and urgently needs your help." Internet: http://www.zdnet.com/article/mozilla-the-internet-isunhealthy-and-urgently-needs-your help/, Jan. 20, 2016 [Feb. 16, 2018]

[15] M. Prokin, "Qualification form for GPRS terminal manufacturer registration." Internet: http://www.dmdm.rs/PDF/FUT/FUTKval Formular.pdf, Apr. 26, 2005 [Feb. 16, 2018]

[16] Beyond the hype: Blockchain in capital markets, http://www.mckinsey.com/industries /financial-service/ourinsights/beyond-the-hype-blockchains-in-capital-markets

[17] Blockchain Adoption Moving Rapidly in Banking and Financial Markets: Some 65 Percent of Surveyed Banks expect to be in Production in Three Years, https://www03.ibm.com /press/us/en/press release/50617.wss

## BIOGRAPHIES

**BOBBY K SIMON,** received the Bachelor's Degree in Computer Science and Engineering from Karpagam University, TamilNadu, India in 2017. He is currently pursing Master's Degree in Computer Science and Engineering in Sree Buddha College of Engineering, Kerala, India. His research area of interest includes the field of internet security, data mining and technologies in Department of Computer Science and Engineering.

**ANJANA P NAIR,** received the bachelor's degree in LBS Institute of Technology for Women, Kerala, India. And master's degree in Computer Science and Engineering from Sree Buddha College of Engineering, Kerala, India in 2013. She is a lecturer in the Department of Computer Science and Engineering, Sree Buddha College of Engineering. Her main area of interest is Core Computers and has published more than 10 referred papers.