ELECTRONIC VOTING SYSTEM VIA GSM

Kabandana Innocent[1], UwitonzeAlfred[2]*
[12]Kigali Independent University ULK, School of Science and Technology, Computer Science Department
[*]Corresponding author Email: kabandanainnocent2020@gmail.com

ABSTRACT

Voting is a right for every citizen allowed to vote in democratic countries. Different countries are having manual or electronic systems to elect their Constitutional Law and their different leaders like President, Prime minister, Member of parliaments, senates, etc. Electronic Voting System via GSM will provide additional facilities to the voters and candidates, to make election more flexible and efficient compare to the traditional election. We will use Global System for Mobile Communication to facilitate the candidates and voters to use this technology to register, elect their candidates from their places and the total votes will be published in a very short time period. This system is capable to enhanced voter verification and mobility while maintaining voter privacy with One Time Password (OTP) generation. Our main objective is to design a secure GSM Mobile Communication Electronic Voting (GMC-EV) model to establish secured connectivity and One Time Password (OTP) based authorization during GSM based electoral process to enhance the authentication of the system. We will use Software Development life Cycle model as our methodology to implement our Electronic Voting System via GSM. The key findings is the test bed simulation of the proposed GSM-Electronic Voting System, the other key findings include the comparison of the time analysis of Secure Hash Algorithm 1(SHA-1) and Secure Hash Algorithm 2(SHA-2). Our system will based on GlobalMobile Communication Electronic Voting as different people are now having smart phones, One Time Password will be generated for every voter. As a recommendation, the Election Commission of Voting System should train the key parsons who will make the *follow up, different activities of the elections from the beginning to the end of the election.*

Key words: ***GMC-EV, OTP, Secure Hash Algorithms, GSM-SMS, IMEI***

1. INTRODUCTION

Elections have a long history, different countries in the world use different methods for voting the leaders. In a Democratic country elections are considered as the key factors for the development of the nation as it provides the voter with opportunity be a part of the policy making and country building. The process of election involves co-ordination of different mechanisms involving the registration of the voter, candidates and examining the information provided by the voter as well as candidates. Selecting the information, maintaining confidentiality of the information, conducting a free and air election turns to be a tedious process. To have a free and fair election no ambiguity in any of the mechanism should be allowed, in failing to do so will fail the motto of the democracy. Overcoming these problems and with the advancement of technology also the need to reduce cost, improve security, efficiency and reduce human interface gave rise to the idea of Electronic Voting (Kabandana, 2016).

This study introduces a secure prototyped GMC-EV for establishing robust and efficient broadband connection between the cell phone (non-smart devices) and centralized server. The proposed GMC-EV intends to perform a secure communication considering communication and Mail Application Program Interface (API) in less congested traffic in wireless channels. As the number of internet users is increasing day by day, it results in a much insecure channel regarding readability, availability and there are intruders who are overhearing to interrupt communication.

The novelty of this paper is as follows: It adopts the concept of Secure Hash Algorithm (SHA-1) and SHA-2 to solve general E-voting issues. If the registered users are not verified properly thus vote given for a particular candidate can be interrupted and manipulated easily by the intruder in a communication channel. The solution presented in this paper is to introduce client and server level encryption and decryption of voter's data using hop based stenography encoding and decoding mechanism SHA value. This paper also conceptualizes a theoretical cryptosystem based on theoretical analysis of SHA-1 and SHA-2 algorithms to accomplish enhanced performance of the proposed system(Neha, 2016).

The proposed OTP based crypto system configured and enabled in both server (GSM/application) and client side which brings out the novelty by reducing the computational complexity and processing time. This paper also highlights how the experimental outcomes are initiated using software and hardware combined prototype model and its significant impact on achieving more security in e-voting systems. Various conventional studies in literature that focused on mitigating security issues associated with electronic voting system but very fewer of them are found to have a notable contribution to improve the performance metrics of the conventional e-voting mechanisms from security aspect (Weldemariam et Adolf, 2010).

The researchers in designing and developing efficient e-voting systems to provide solutions to the existing models irrespective of any design and technical constraints (Lai et al., 2009). Traditional election system is causing many problems in registration of the voters, candidates, more time needed to elect the candidate and count the votes and also there is no trust of the results. Hence, the proposed GMC-EV aims to mitigate the current security issues prevailing in the conventional hardware and software based e-voting system.

This paper further expands the problem identification in the traditional strategies followed by research methodology and algorithm implementations. The algorithm design and mathematical modeling highlight significant impact of OTP generation on a centralized server (GSM based) and the security aspects are measured considering the selection of performance parameters for both SHA-1 and SHA-2 algorithms. The useful performance parameters collection shows how the proposed GMC-EV outperforms conventional hardware/software combined E-voting systems regarding security as well as computational complexity.

2. PROBLEM IDENTIFICATION

This section introduces some of the significant constraints prevailing in the conventional hardware and software based E-voting mechanisms. The conventional GSM-based e-voting systems incorporate various less secure cryptosystems to protect data. It can be seen that scrambling the original data for converting it into another unreadable format makes no sense if the third parties get access to the modified data; as they can easily decrypt it.

It also happens that if the third parties are over hearing the communication channel during the data transmission from the sender to the receiver node, they can quickly perform an attack to modify the data. The existing security challenges in GSM based

E-voting system make it more susceptible to the attacks such as rotation, translation, etc (Yang et al., 2006). To mitigate the above-mentioned issues, our paper adopts the concept of OTP generation along with performance of SHA-1 and SHA-2 hash algorithms to protect the sender and receiver authorization in the wireless channel.

Therefore, it is essential to formulate a robust authentication mechanism which can be further emerged with the conventional hardware and software combined E-voting technologies. MatejTravnicek et al. suggested that the implementation of E-voting considering secure wireless medium and embedded electronics only can accomplish success, if it is deployed into the system as per the electoral need (MatejTravnicek et al., 2012). However, the overall process for election is almost the same, but it differs from country to country in terms of complexity, system installation and cost (Lauer et al., 2004). The installation of contactless Integrated Circuit (IC) for E-voting and its integration poses vulnerability on the communication medium.

3. RESEARCH METHODOLOGY

The aim of this research is to design a secured GSM communication based E-voting mechanism which mainly obtains web security by integrating secure Hypertext Transport Protocol (HTTPS) with the Application Program Interface (API). The proposed system also initiates HTTPS to work with encrypted Secure Socket Layer (SSL) transport mechanism. The SSL also provides an efficient interactive and reliable end-to-end security services to the higher layer protocols of Open Systems Interconnection (OSI) model such as Transmission Control Protocol/Internet Protocol (TCP /IP) and many application and presentation layers protocols. SSL services use the concept of Rivest, Shamir and Adleman(RSA) for exchanging RSA session keys over the transport and session layers for authenticating the session keys (NaQi and or &, Wei Wei, 2013).

The proposed system also incorporates RSA-based encryption technique which further activates Message Authentication Code (MAC) to further provide secure message integrity over higher layer protocol like HTTP. The HTTP socket layer basically allows the GSM server side and the client's mobile side to verify the communication channel by a negotiation over MAC algorithm and session keys to protect the one-time session. The SSL handshake protocol mainly includes 4-phases client and server level authentication stages to establish a secure communication using HTTPS client and server side socket. However, various conventional studies previously initiated the Transport Layer Security (TLS) script on authenticating the client and server based communication scenario but the broad applicability of SSLv3.3 makes it appear totally efficient as compared to the conventional TLS (Thyla van der Merwe,2018).

The proposed system uses SSLv3.3 for authentication of phase 2 and phase 3 where server may send certificate, exchange key objects and validate transmitted client hello signals in terms of certificate and server key exchange processes. The following diagram shows the tentative system architecture of the proposed GSM (centralized server) based communication scenario.

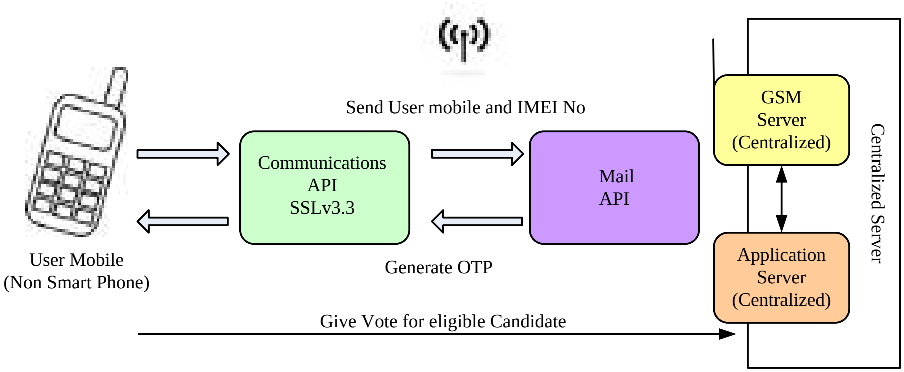

Figure 1: Proposed GSM based Secure E-voting Architecture

The above figure1 shows how a voter can be validated for giving a vote to a particular candidate stood for election. The proposed system validates a user device by tracking its International Mobile Equipment Identity (IMEI) number. Initially, the voter provides its user mobile number and unique IMEI number to the centralized server using client interface system.

The communication API establishes a communication ~~in~~ between the GSM server and the application server to check whether the voters IMEI number and mobile number exists in the election commission's online database or not, if it exists then it will encrypt the IMEI number and phone number using the proposed GMC-EV. It further encrypts the IMEI and phone number and initiates a ‘HELLO' message from the GSM communication port. If the receiver end receives the HELLO message, then it requests to the server for OTP. The GSM server then generates the OTP and acknowledges it to the cellular device (voter). The voter authenticates itself by providing the same OTP to the GSM server and gives vote for the eligible candidate. The proposed system uses the following modules for client mobile IP authentication process:

a. One-Time Password Generation by GSM Server

The proposed system exploits fully the OSI model where the media access control layer and logical link control (LLC) layer encodes and decodes the transmitted data packets into logical (0 to 1) representation. The data link layer also provides a mechanism for error minimization and well synchronization in the transmission channel. It also provides an interactive solution to map the physical address of GSM device ports into link layer data frames for good synchronization. The proposed system also activates GSM server to initialize OTP to provide better security aspects into client authentication module. Therefore, the random generation of OTP from GSM server makes client authentication process very invulnerable to any malicious network attacks (Sagar, 2013).

It appears to be very effective as the server generated OTP can be used only once, and the session layer expires session on the delay of providing the received OTP and its respective verification process by the GSM server module. As the OTP generation concept considered as invulnerable to any passive attacks and sniffing thus it poses better security aspect. The proposed system also introduces a unique mathematical algorithm to represent the OTP generation process by GSM server which depicts well time-synchronization between the authentication server and client e.g. voter. The random number generation procedure is further fed into a one-way function.

b. Integration of Secure hash functions into the proposed system

The proposed GMC-EV is designed by adopting the non-invert ability of a safe hash function. It defines relatively the easiest way to compute the hash based data in a forward direction but poses computationally inefficiency to the invert notion. The proposed system also enables SHA-1 and SHA-2algorithm at the server side where a hash function $h_f$takes a variable length message m and convert it into fixed length $h_f(m)$ SHA-2. The proposed GMC-EV applies the SHA as a hash function relatively pretenses better security aspects as compared to the conventional ones. The notable properties of the hash function are:

- It can be applied to variable length data sizes.
- It produces a fixed length message digest.
- h_f (m) depicts ease of computation for any variable length messages considering both hardware and software combined systems in real time.
- The security features of SHA algorithm highlights that it is computationally infeasible to find the value of original message m after converting it into a message digest of fixed length such that $h_f (m) \rightarrow M$
- The one-way property of hash algorithms also makes it computationally infeasible to find the original message $m \neq n$ while $hf (m) = h_f (n)$.

- The SHA algorithm also known for strong collision resistance as technically it is not feasible to find any pair (m, n) such that h_f (m) = h_f (n).

The above-mentioned are the characteristic features of secure hash algorithm by its one-way features and high cryptosystem formulation.

- **SHA-1 Secure Hash Function**

The secure hash algorithm is used in the proposed GMC-EV model. In this proposed system, SHA-1 takes input message as a 2^{64} bits data and produce 150 to 160 bit message digest. The message digests produced by the SHA-1 consists of fixed length output (Harshvardhan Tiwari, 2010).

c. Message Authentication Code

The proposed GMC-EV model also adopted the concept of Message Authentication CodeMAC for protecting/encryption GSM generated OTP. Basically, the intruders can overhear the channel and perform active attacks, i.e. falsification of data and transactions. The use of MAC, basically integrated into the proposed GMC-EV helps to verify the sender and the content of the data packet being transmitted through the channel. The proposed system uses the above-stated cryptosystems on GSM server module, which minimizes the probability of passive attacks in the transmission medium (channel) (Jerone B. Alimpia, 2018). Since sometimes the long encryption process to encapsulate the data increases the use of resources and complexities thus there is a need for data packet authentication irrespective of data encryption.

4. PROPOSED GSM ARCHITECTURE AND TECHNICAL SPECIFICATION

This section introduces the GSM network architecture which is embedded into the proposed system. The most prominent features and its respective detailed description are discussed 4.1.

4.1 Architecture

As GSM communication is considered as one of the most widely used telecommunication technologies in the modern world, it is further incorporated in the proposed GMC-EV system. It also has been utilized in the systems like Universal Mobile Telecommunications System (UMTS). The design specifications and its important features are discussed below.

In the proposed system, the client side uses a non-smart phone which consists of the following two parts:

a. **Mobile Device/Handset:** The proposed system uses a mobile device on the client side to communicate with the server for E-voting purpose. By using the handset, the mobile device can receive the OTP and it can give a vote for the eligible candidate.

b. **Subscriber Identity Mobile (SIM):** The SIM which is a portable chip contains two types of user information which are as follows.

- Subscriber Identity
- Subscriber Authentication Information

The subscriber authentication information associated with the proposed GSM kit contains the International Mobile Subscriber Identity (IMSI). IMSI number is defined in a way where it is a unique number for each subcarrier. The IMSI number includes the unique identity of the sub carrier in the network as well as it also contains the information of the home or the country network.

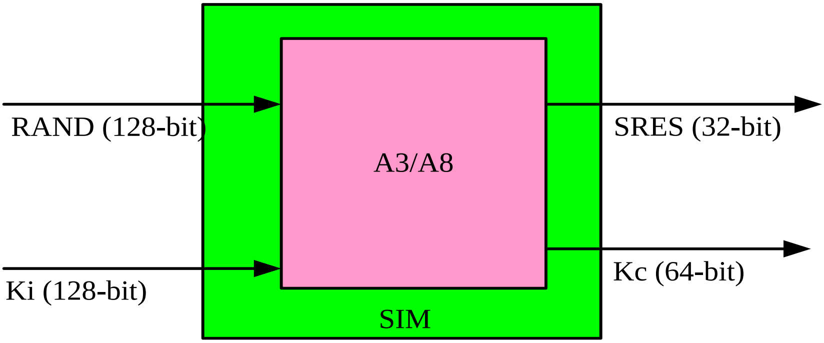

Figure 2: GSM SIM Architecture for the proposed E-voting system

The proposed GMC-EV system considers a Ki encryption parameter. The GSM SIM randomly generates 128-bit number and allocates it to the particular subscriber. All the keys and challenges are further stored into the GSM server. The SIM internal design is highlighted in figure 2 and it shows that it plays a crucial role during the authentication process of user and how it generates the OTP for each user. It can also be seen that the signal transmission through wireless medium only happens when the

SIM is inserted into the GSM module, and it activates the services for online process. The random number is initiated and process through the communication channel to the mobile station. The SIM also performs the same operations during the signal transmission. The Signed Response (SRES) which is computed initially is compared with the current SRES by the network. If they match in both the client and GSM server side, then it is said that the SIM is authenticated.

4.2 International Mobile Equipment Identity

The proposed system also incorporates tracking of voter's non-smart phone (IMEI) number which is unique to every user. The IMEI number of the mobile phone is connected to the GSM network and stored in a database namely Equipment Identity Register (EIR) contains all the valid mobile phone equipment.

4.3 GSM-SMS

The proposed GMC-EV system also initiates GSM based SMS to establish communication in between the client and server. The SMS over GSM network uses message length up to maximum 160alphanumeric characters and cannot contain any image or graphic object files. The reason, GSM service is integrated into the proposed GMC-EV system got high data speed, cheap rates and guaranteed the successful transmission of data packets. The Short Message Service Center (SMSC) handles the message transmission in case the cellular device is switched off and tracks down the transmission until and unless the message reaches its destination. SMSC relays the data packets to the appropriate receiver by locating its coordinates on Home Location Register (HLR). If the receiver is out of coverage, SMSC store the message into its database, by the time the receiver becomes active and comes within coverage range the HLR immediately notifies the SMSC. The following figure 3 shows the GSM message delivery services.

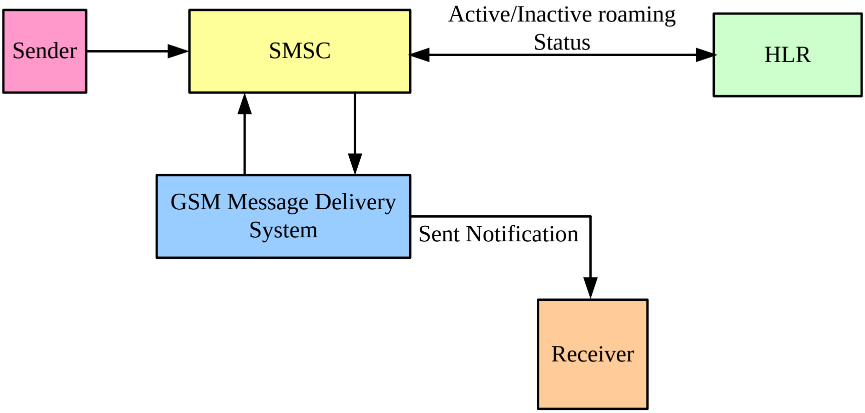

Figure 3: GSM SIM Message Delivery System

4.4 Extensible Authentication Protocol (EAP)

As highlighted and discussed in the previous part, there are some security contemplations with the GSM framework. One approach to enhance the safety in GSM is to utilize it together with the Extensible Authentication Protocol (EAP). By doing this both 2-ways confirmation and more grounded end-to-end security can be figured ~~it~~ out. This part exhibits the EAP which is characterized in the RFC3748 and the detail for use in versatile situations described in RFC4186EAP-SIM (2006). EAP is a verification system which underpins various confirmation strategies. It regularly runs specifically over joint information layers, for example, Point to Point Protocol (PPP) or IEEE 802, without requiring IP. EAPwas initially expected to be utilized over PPP, yet has additionally been received by the IEEE 802.11i standard.

- **Types of EAP Messages**

EAP uses four types of messages. These are:

– Request: Messages sent from the authenticator to the supplicant
– Response: Messages sent from the supplicant to the authenticator
– Success: Sent from authenticator when access is granted
– Failure: Sent from authenticator when access is denied

4.5 ALGORITHM IMPLEMENTATION STRATEGIES

The proposed GMC-EV is designed considering hardware and software application based the combined system. The hardware is a GSM tool embedded with a centralized server running a software application on the back end.

Algorithm One: Admin Module running on a Centralized Server | Add Voter/User

Input: η (A_{ID} Y A_{PASS}).

Output: Add V_i, Declare Election Schedule (E_s), Election Results (E_R)

```
Start

Step 1: Initialize $A_{ID}$, $A_{PASS}$, $V_i$, $U_i$, $\eta_{Server}$

Step 2: if (login == 1)

Step 3: Activate $\rightarrow A_{Module}$
Step 4: for (i $\leftarrow$ 1: n)
Step 5: Add $\leftarrow V_{i\{\text{Name, Email, Mobile, Password, IMEI No}\}}$
Step 6: If (Successful)
Step 7:  Generate $\leftarrow V_{ID}$
Step 8: Add $\leftarrow V_i$
Step 9: Declare $\leftarrow E_S \mid E_{R.}$
```

End

The above-mentioned algorithm shows the mode of admin module communication with centralized server and it adds voters. Firstly admin logins into election commission system database to gain access to the application server. η (A_{ID} Y A_{PASS}) signifies a function which denotes that admin should enter it's respective Admin ID (A_{ID}) and password (A_{PASS}) login into the centralized system (web server). Voter, user, and centralized application server are denoted by the variables V_i, Ui,$\eta_{Server.}$

Algorithm Two: Admin Module running on a Centralized Server | Add Candidates

Input: η (A_{ID} Y A_{PASS}).

Output: Add C_i, Declare Election Schedule (E_s), Election Results (E_R)

Start

```
Step 1: Initialize $A_{ID}$, $A_{PASS}$, $C_i$, $U_i$, $\eta_{Server}$
Step 2:  for (i $\leftarrow$ 1:n)
Step 3: If ($V_{IDi}$! = Exist in Application Database)
 Step 4: Add $\leftarrow V_i$
Step 5: Else
Step 6: Register $\leftarrow C_{i\{\text{Party Name, Name, Email, Mobile, Password, Election Type}\}}$
Step 7:  Declare $\leftarrow E_S \mid E_R$
```

End

Algorithm Thee: Election Results (E_R)

Input: η (A_{ID},A_{PASS}).

Output: Declare Election Schedule (E_s), Add C_i, V_i, Election Results (E_R)

Start

```
Step 1: Initialize $A_{ID}$, $A_{PASS}$, $C_i$, $U_i$, $\eta_{Server}$
Step 2: Election Schedule $\leftarrow$Admin
Step 3:  for (i$\leftarrow$ 1:n)
Step 4: If ($V_{IDi}$!= Exist in Application Database)
Step 5: Add $\leftarrow V_i$
Step 6: Else
Step 7: Register $\leftarrow C_{i\{\text{Party Name, Name, Email, Mobile, Password, IMEI, Election Type}\}}$
Step 8: Declare ←$E_S$
Step 9: Voting process ←$V_i$
Step 10:Result← $E_R$
End
```

Algorithm two and three, depict how a candidate can be registered considering its voter ID by the centralized web server. It also checks whether a voter who is nominated for candidate position still exists in the centralized database or not. If it exists, the algorithm will add that voter as candidate else it will notify the person to register himself as a voter again. The proposed system also incorporates a GSM server which communicates with the web server and the mobile phones using communication interfaces API.

- **Integration of Communication API into the Proposed System**

Java communication API version 3.0 enabled as an extension. It is a tool which defines a set of instructions that perform a specific communication in between two different units through a wireless channel medium. The proposed E-voting mechanism incorporates the Java communications API as a platform-independent tool, embedded with both sender and receiver end GSM system.

Functional Aspect

In this paper, the java communication API namely Javax.com provides an application independent interface GSM RS hardware serial ports which are denoted by COM1, COM2, COM3, etc. It provides very limited access for data transfer to the parallel ports of RS GSM hardware modules (IEEE-1284).

The proposed system enables *Service Switching Point*(SPP) mode in GSM RS-232 hardware module where the implementation of the data transfer process has been carried out using Solaris Scalable Processor Architecture (SPARC), Solaris x86 and Linux x86. The proposed client's product line is configured with the port mapping extensions of the GSM kit to allow the admin module for specifying the port locations as well as their visibility regarding names and annotated references.

API serial features

Following are the API serial features used for the implementation of GSM based E-voting system.

- Count of ports (supervisor and client configurable port mapping)
- Port arrangement (baud rate, speed, stop bits, equality)
- Access to EIA232 standard *Data Terminal Ready*(DTR), *Code Division* (CD), *Cordless Telephone System* (CTS), *Radio Technology Somfy*(RTS) and *Data Set Ready* (DSR) signals
- Exchange of information over RS-232 ports
- Equipment and programming stream control choices
- Get cradle edge control

- Offbeat occasion choice for warning off:
- Information accessible on a RS-232 port
- Port equipment line level changes
- Port possession changes inside a solitary Java Virtual Machine (JVM)

Integration of Mail API into the Proposed System:

The admin module software application running on the centralized server back end integrates another built-in package named as Mail API interfaces. It is used in composing, write and read electronic messages for both sender (voter’s mobile) and receiver (centralized server) modules. It provides a platform independent interface framework which can process a set of instructions for sending and receiving SMS.

The proposed system primarily incorporates two different types of packages which are javax.mail and javax.mail.event activation packages respectively. These packages encapsulate the core classes of mail API. It also facilitates the centralized server admin module by registering the voters and the candidates. Mail API core classes used in the proposed system for establishing secure and reliable communication in between the centralized application server and GSM server. Moreover, it is also extended to the user mobile and server communication establishment based on cell phone IP.

The following figure 4 represents the sequence diagram of the proposed GMC-EV model. It also shows how the message transmission through a wireless link has been carried out with respect to time (t).

Figure 4: Proposed E-voting Mail Interface Sequence Diagram

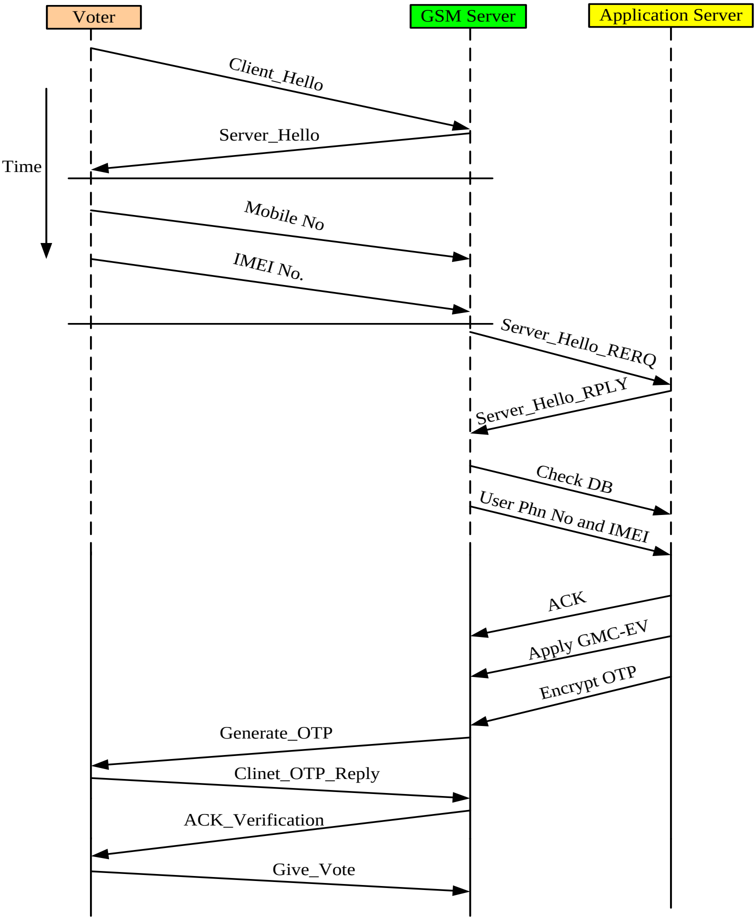

Table 1: Experimental test bed results

5. RESULTS AND DISCUSSION

This section discusses the important findings obtained from the test bed simulation of proposed GMC-EV system. It also highlights a comparative analysis performed, considering the (processing /computation) time of conventional SHA-1 and SHA-2 algorithms. The timing analysis of SHA-1 and SHA-2 depicts that SHA-1 achieves very less processing time and higher security aspects as compared to the conventional SHA-2. Hence, SHA-1 can easily be integrated into the proposed GSM-EV model. The experimental prototyping also shows the ease of computation of proposed GSM-EV model and its extensive applicability into non-smart phones, because if it's much feasibility and robustness. The light weight and easy implementation features make it more attractive as compared to the conventional E-voting systems (i.e. conventional GSM based Intelligent Polling System). The following table highlights the outcomes of the timing analysis obtained from the experimental test bed.

File Size (KB)	**Computation Time (Sec)**	
	SHA-1	SHA-2
10	0.126	0.342
15	0.387	1.154
20	1.285	3.675

Table 2: Impact of Processor on Execution Time

The above table also highlights how SHA-1 achieves very less computation time (sec) with the increment of file size as compared to theSHA-192. The following table 2 shows the manual calculation of execution time regarding processing speed and iterations for conventional systems and the proposed GMC-EV model. The calculation has been carried out considering a test bed simulation for core i3, i5, and i7 CPUs. It shows that the proposed GMC-EV takes fewer resources during the computation and poses very less execution time as compared to the current e-voting applications. The comparative analysis of execution time is highlighted in the following table 2 and 3.

Iterations	**EXECUTION TIME**					
	Conventional Intelligent Polling System			Proposed System		
	Core-i3	Core i5	Core-i7	Core-i3	Core i5	Core-i7
35	0.724	0.633	0.411	0.047	0.021	0.012
110	0.755	0.656	0.419	0.063	0.024	0.012
160	0.736	0.658	0.435	0.080	0.036	0.014
250	0.757	0.689	0.477	0.092	0.048	0.019
320	0.778	0.694	0.481	0.109	0.056	0.023
370	0.809	0.752	0.521	0.125	0.064	0.028
480	0.810	0.753	0.521	0.146	0.069	0.035
530	0.811	0.764	0.535	0.157	0.072	0.039

580	0.812	0.788	0.552	0.174	0.072	0.044
650	0.813	0.797	0.569	0.187	0.077	0.048
760	0.934	0.802	0.578	0.209	0.081	0.055
1100	0.995	0.838	0.588	0.262	0.093	0.061

Iterations	**EXECUTION TIME**	
	Existing System	Proposed System
30	0.727	0.047
100	0.754	0.063
170	0.734	0.080
240	0.756	0.092
310	0.771	0.109
380	0.800	0.125
450	0.809	0.146
520	0.831	0.157
590	0.8705	0.174
660	0.872	0.187
730	0.936	0.209
1000	0.994	0.262

Table 4 shows a comparative analysis of the proposed system with touch screen system where the performance parameters are

considered as processing time in seconds and iterations. It also depicts how the proposed GMC-EV model performs better than the Touch screen E-voting systems.

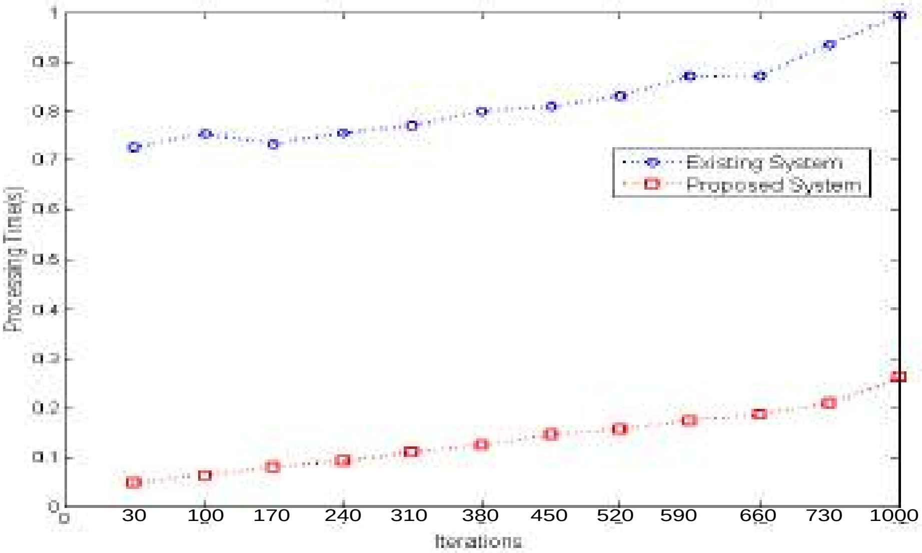

Figure 4: *Resultant Outcomes of Processing Time*

6. CONCLUSION

This paper presented the proposed GSM based secure e-voting system, specified as GMC-EV system and its significant impact on enhancing the security features of GSM communications over wireless channels. This topic also highlights the mathematical algorithms depicts the proposed GMC-EV design theoretically. The experimental outcome shows that the proposed GMC-EV performs better than the Touch Electronic Voting System.

REFERENCES

Kabandana Innocent and A.N.Nanda Kumar (2016), *FPF: Fraud Proof Framework for Electronic Voting System,* International Journal of Electrical and Computer Engineering (IJECE) Vol. 6, No. 3, pp. 1197 ~ 1204.

Neha Kishore, Member IAENG, and Bhanu Kapoor (2016), *Attacks on and Advances in Secure Hash Algorithms*"IAENG International Journal of Computer Science".

Lai, J. Y., Lin, C. F., & Yang, C. H. (2009),*Design and Implementation of an Electronic Voting System with Contactless IC* Cards. Graduate Institute of Information and Computer Education, National Kaohsiung Normal University.

Li, Chun-Ta, and Min-Shiang Hwang (2012), "*Security enhancement of Chang-Lee anonymous E-MatejTravnicek voting scheme*." International Journal of Smart Home 6, no. 2: 45-52.

Lauer, Thomas W (2004), "*The risk of E-voting*" Electronic Journal of E-government2, no. 3: 177-186.

IETF, RFC 4187 (2006), "*Extensible Authentication Protocol Method for Global System for Mobile Communication (GSM) Subscriber Identity Modules* (EAP-SIM)", Jan, 2006

NaQi , Wei Wei*et al.*(2013), *Analysis and Research of the RSA Algorithm*, "Information Technology Journal", 1818-1824.

Thyla van der Merwe (2018),*An Analysis of the Transport Layer Security Protocol*, (2018)

Sagar Acharya, ApoorvaPolawar, P.Y.Pawar (2013), *Two Factor Authentication Using Smartphone Generated One Time Password*," IOSR Journal of Computer Engineering", PP 85-90

Harshvardhan Tiwari, Dr. Krishna Asawa (2010), *A Secure Hash Function MD-192 With Modified Message Expansion*, "International Journal of Computer Science and Information Security"

Jerone B. Alimpia, Dr. Ariel M. Sison2, and Dr. Ruji P. Medina (2018), *An Enhanced Hash-based Message Authentication Code using BCrypt*, " International Journal for Research in Applied Science & Engineering Technology".

Weldemariam et Adolf (2010), *Electronic Voting Development and Trends*.